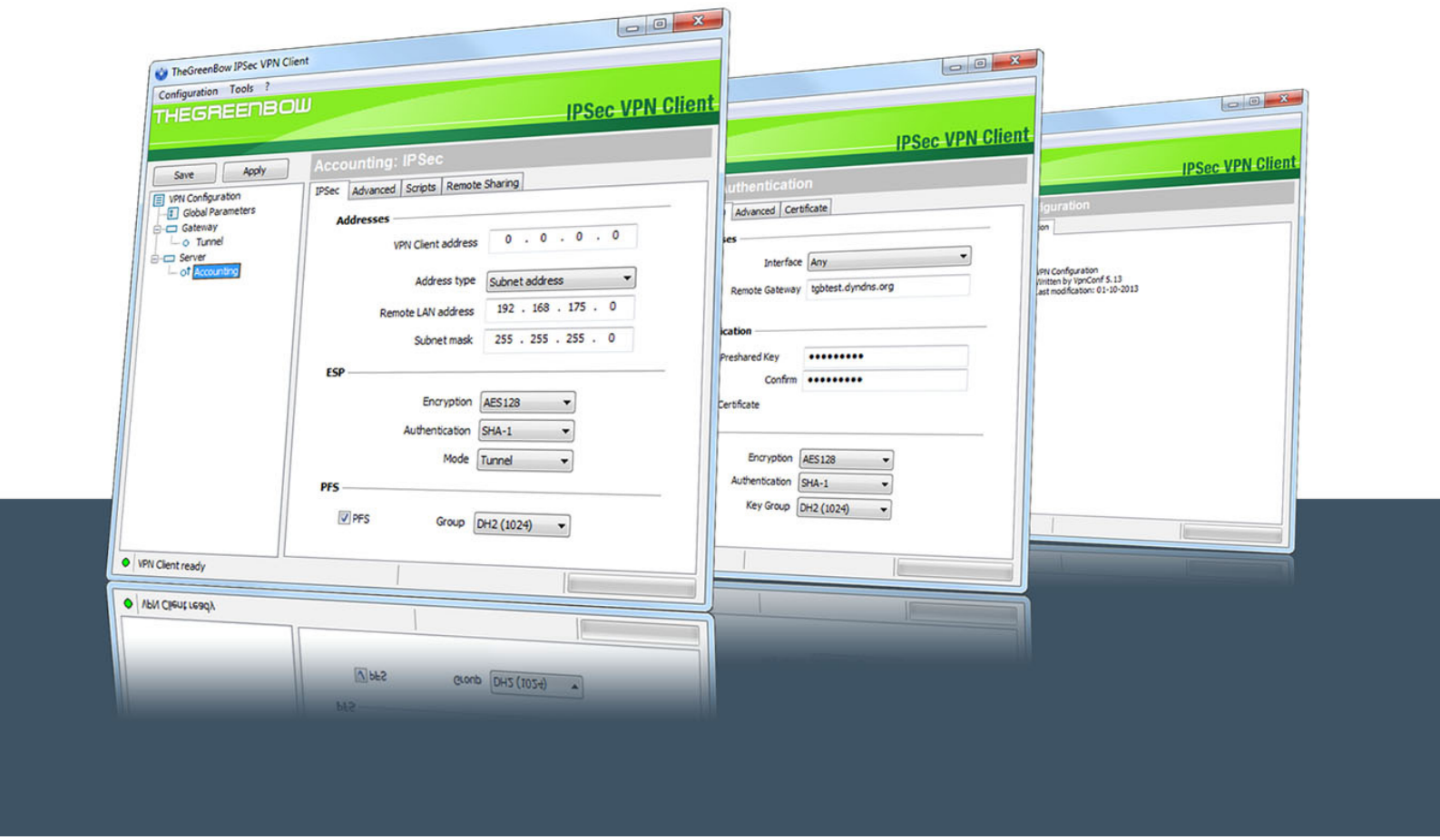


TheGreenBow VPN Client

User Guide

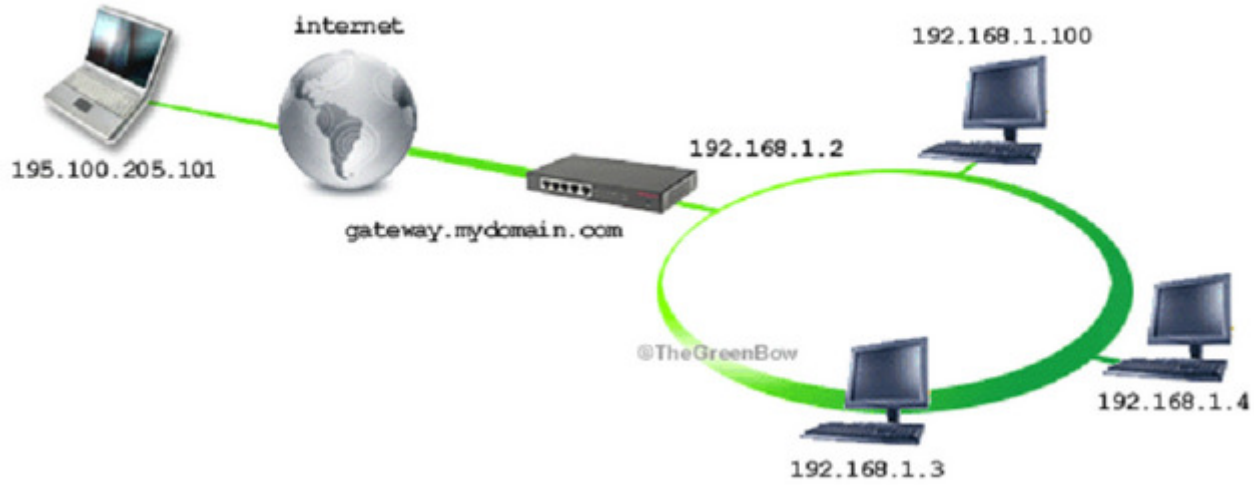
Table of Contents

1 Presentation

1.1 The universal VPN Client

TheGreenBow VPN Client is a VPN Client software designed for any Windows workstation or laptop. It establishes a connection, and guarantees a secure communication with the information system of the company.

TheGreenBow VPN Client is universal and compatible with all IPsec VPN gateways on the market (see the list of qualified VPN gateways). It also helps to establish VPN tunnels in point-to-point connection between two machines equipped with the software. TheGreenBow VPN Client implements IPsec, IKE and SSL standards to be compatible with openVPN Gateway.



For most VPN gateways on the market, TheGreenBow provides a configuration guide. To configure your VPN gateway, see the list of configuration guides of VPN gateways.

1.2 Full compatibility with PKI

TheGreenBow VPN Client is fully integrated in all PKI (Public Key Infrastructure). He brings unparalleled flexibility in taking account of certificates and Smartcards:

- Compatibility with a wide range of Token and Smartcard (see list of qualified Tokens)
- Automatic detection of smartcard and token (PKCS11 or CSP) or storage media (file, Windows certificate store)
- Configuring Tokens "on the fly"
- Taking into account multi-format certificates (X509, PKCS12, PEM)
- Configuring multi-criteria certificates to be used (subject, key usage, etc...).

TheGreenBow VPN Client offers more features with additional security around the PKI management, such as the opening and closing of the tunnel upon insertion and removal of the Smartcard, or the ability to configure the PKI interface and Smartcard in the installer software, to automate deployment.

1.3 VPN security policies

TheGreenBow VPN Client provides a high level of security management and the consideration of VPN security policies.

The software can be configured when installed to restrict all access VPN security policies the administrator only.

The software also allows you to secure the maximum use of VPN security policies, conditioning the opening of a tunnel to the various authentication mechanisms available: X-Auth, certificates...

1.4 TheGreenBow VPN Client features

TheGreenBow VPN Client provides the following features:

- Ability to support network in IPv4 and IPv6 simultaneously
- Ability to create IPsec VPN tunnel using either IKEv1 or IKEv2
- Ability to create VPN tunnel using either IPsec or SSL
- Multiple VPN tunnels with a mix of IPsec and SSL
- Point-to-point or peer-to-gateway IPsec VPN tunnel
- VPN Tunnel on all media types: Ethernet, WiFi, 3G, satellite
- Support of PKI, and gateway or user certificate management
- Taking into account Smartcards or tokens, and Windows certificate store
- User mode (limited), Director (VPN Security Policy Management) and USB (roaming)
- Open tunnel automatically and GINA mode
- X-Auth Authentication static or dynamic
- "DPD" (Dead Peer Detection) features and automatic failover the tunnel to a redundant VPN gateway
- Mechanisms for maintaining the VPN tunnel in unstable network
- IP filtering unauthorized flows (firewall feature)

See chapter "TheGreenBow VPN Client specifications".

2 Software

2.1 Installation

2.1.1 Installation

Installing TheGreenBow VPN Client is done by running the program:

TheGreenBow_VPN_Client.exe

The installation is a standard procedure that requires no user input.

Note: The performance of the system is configurable using a list of command line options, or by using an initialization file. These options are described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

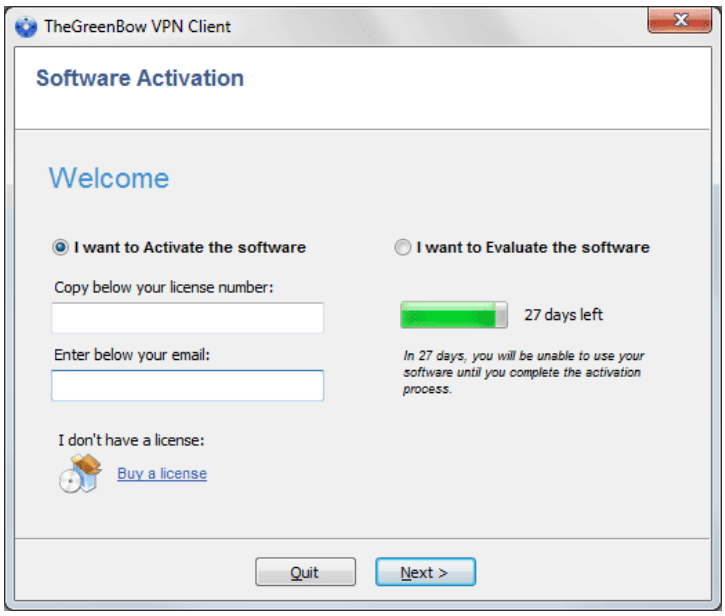
2.1.2 Installation requirements

See chapter "TheGreenBow VPN Client specifications" for supported OS.
Installation on Windows XP, Windows Vista, Windows 7 and Windows 8 needs to be in Administrator mode the computer.
When this is not the case, a warning message notifies the user and the installation stops.

2.1.3 Evaluation period

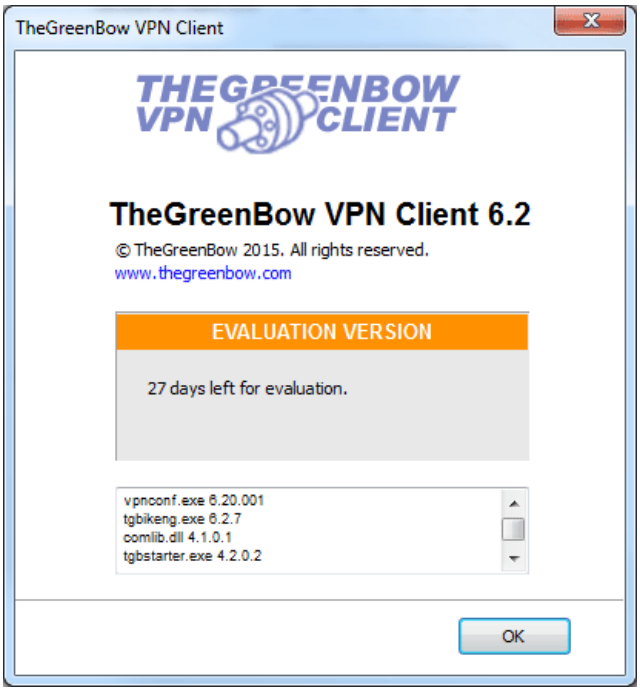
At its first installation on a machine, the VPN Client is in evaluation period of 30 days. During the evaluation period, the VPN Client is fully operational: all features are available.

Each time the software is launched, the activation windows is displayed. It shows remaining number of days for evaluation.



For further evaluation of the software, select "I want to evaluate the software" and then click "Next>".

During the evaluation period, the "About..." window displays the remaining number of days for evaluation:



During the evaluation period, it is always possible to directly access the software activation via the menu: "?" > "Activation Wizard..." from the Configuration Panel.

2.2 Activation

The VPN Client must be enabled to operate outside of the evaluation period.
The activation process is accessible either each time the software is launched or via the menu "?" > "Activation Wizard..." from the Configuration Panel.

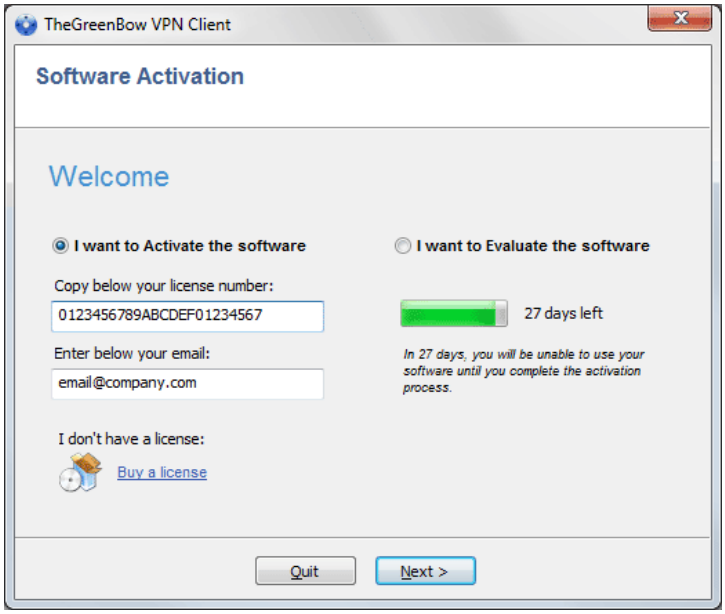
The activation process is a two-step procedure.

2.2.1 Step 1

Enter the license number received by email in "Copy here your license number". To get the license number, click on "Purchase license".

The license number can be copied and pasted directly from the email in the field. The license number is composed solely of characters [0 ... 9] and [A.. F], possibly grouped by 6 and separated by dashes.

Enter in the field "Enter your email address:" The email address identifying your activation. This information allows to recover in case of loss, information about your activation.



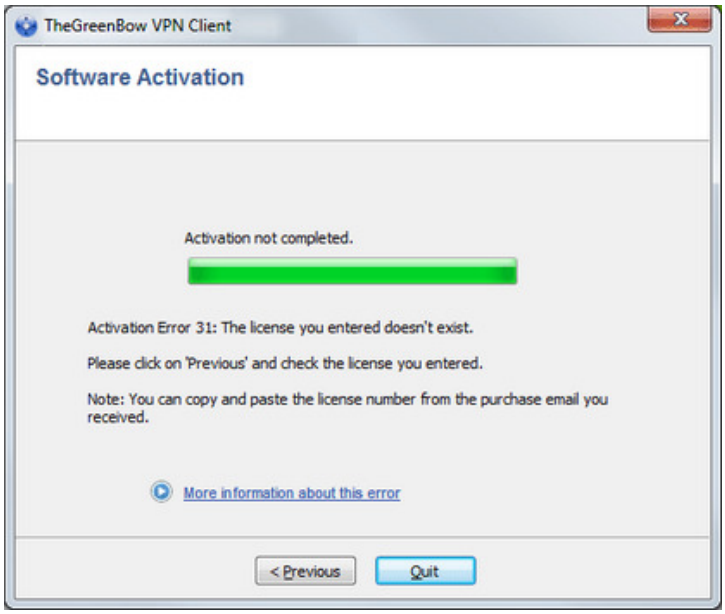
2.2.2 Step 2

Click "Next>", the online activation process runs automatically. When activation succeeds, click "Start" to start the software.

Note: The software activation is linked to the computer on which the software is installed. Thus, a license number which allows only one activation cannot to be reused on another computer, once activated.
Also, the activation of the license number can be reset by uninstalling the software.

2.2.3 Activation errors

Activating the software might fail for different reasons. Each error is indicated on the activation window. It is possible that a link provides information, or offers a way to fix the problem.



All activation errors, as well as procedures to solve the problem of activation are described on the TheGreenBow website at: www.thegreenbow.com/support_flow.html?product=vpn

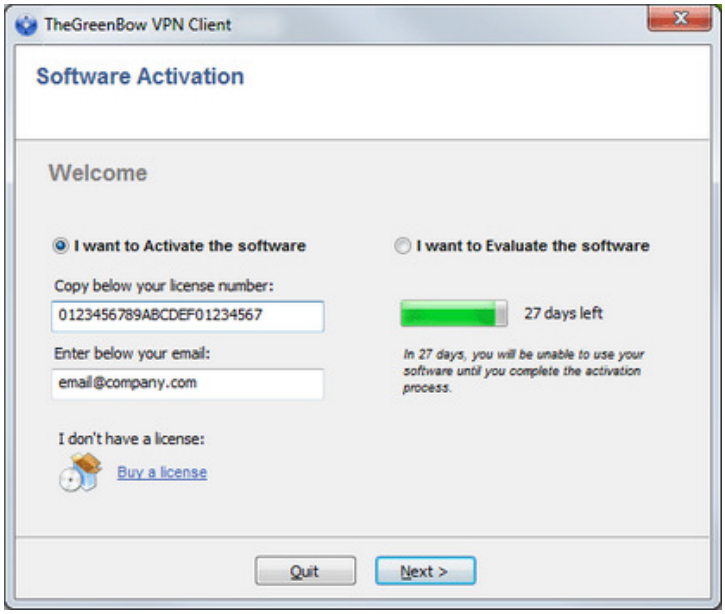
Activation errors that are the most common ones include:

No	Meaning	Resolution
31	The license number is not correct	Check the license number
33	The license number is already activated on another computer	Uninstall the computer on which the license has been activated, or contact TheGreenBow sales team
53 54	Communication with the activation server is not possible	Check the extension is connected to the Internet Check the communication is not filtered by a firewall to a proxy. If applicable, configure the firewall to let the communication, or the proxy to redirect it correctly.

2.2.4 Temporary license

It is possible to acquire from TheGreenBow evaluation licenses, called temporary licenses, in order for example to continue testing sessions beyond the standard evaluation period. To obtain a temporary license, contact the sales department by mail: sales@thegreenbow.com.

During the use of a temporary license, the activation window is always displayed when the program starts. An icon identifies the license is temporary, and the number of days remaining is displayed.



To launch the software, click on "Next>". At the end of the period of validity of the temporary license, the software must be activated by a full license for further use.

2.2.5 Find license and software release number

When the software is activated, the license and the email used for activation are available in the "About..." window of the software.

2.2.6 Manual Activation

If you still have software activation error, it is possible to activate the software "manually" on TheGreenBow website:

1	"prodact.dat" file	On the computer to be activated, retrieve the "prodact.dat" file located in the Windows directory "My Documents". (1)
2	Activation	On a computer connected to the activation server (2), open the manual activation page (3), post prodact.dat file, and retrieve the tgbcode file automatically created by the server.
3	"tgbcode" file	Copy this "tgbcode" file in the Windows "My Documents" of the computer to activate. Launch the software: it is activated.

(1) The file "prodact.dat" file is a text file that contains the elements of the computer used for the activation. If this file does not exist in the "My Documents" folder, do the activation on the computer: even if it fails, it has the effect of creating this file.
(2) The activation server is TheGreenBow server available on the Internet.
(3) See detailed procedures below.

2.2.6.1 Manual activation on the activation TheGreenBow server

Open the following webpage: www.thegreenbow.com/activation/osa_manual.html

Click the "Browse" button and open the "prodact.dat" file recovered on the computer to activate.
Click on "Send". The activation server verifies the validity of the product.dat file information.
Click "Perform".
During download the activation server shows the file containing the activation code used to activate the computer.

This file's name is as follow: tgbcode_[date]_[code].dat (e.g. tgbcod_20120625_1029.dat)

2.3 Software Update

The software allows you to check at any time if an update is available through the menu of the Configuration Panel: "?" > "Check for update". This menu opens the checking update webpage, which indicates whether an update is available and activated, depending on the purchased type of license, as well as on the subscribed type of maintenance. This is also available here: www.thegreenbow.com/latestversion.php

2.3.1 How to obtain an update

The rules to obtain a software update are as follows:

During the maintenance period (1)	I can install any updates
Outside maintenance period, or without maintenance	I can install the minor updates (2)

(1) The maintenance period starts on the first activation of the software.
(2) The minor releases (or maintenance updates) are identified by the last digit of the version, e.g. the "2" of "5.12".

Examples:
I activated the software in 5.12 release. My maintenance period has expired.
All updates from 5.13 to 5.19 releases are allowed.
Updates of 5.20 and above releases are denied.

2.3.2 Update of VPN security policy

During an update, the VPN security policy (VPN configuration) is automatically saved and restored.

Note: If access to the VPN security policy is locked by a password, this password is required during the update, to allow the configuration recovery.

2.3.3 Automation

Performing an update is configurable using a list of command line options, or by using an initialization file. These options are described in the "VPN Client Deployment Guide" (VPN Standard: tgbvpn_ug_deployment.pdf, VPN PREMIUM: tgbvpp_ug_deployment.pdf).

2.4 Uninstalling

To uninstall TheGreenBow VPN Client:
1/ Open the Windows Control Panel
2/ Select "Add / Remove programs"

or

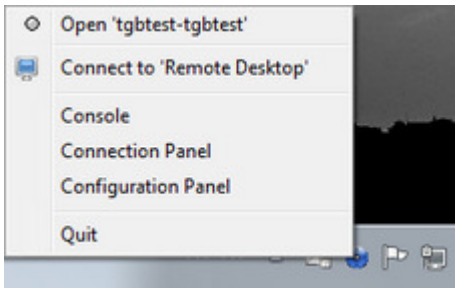
1/ Open Windows menu "Start"
2/ Select "Programs" > "TheGreenBow" > "TheGreenBow VPN" > "Uninstall VPN Client"

3 Quick Use Cases

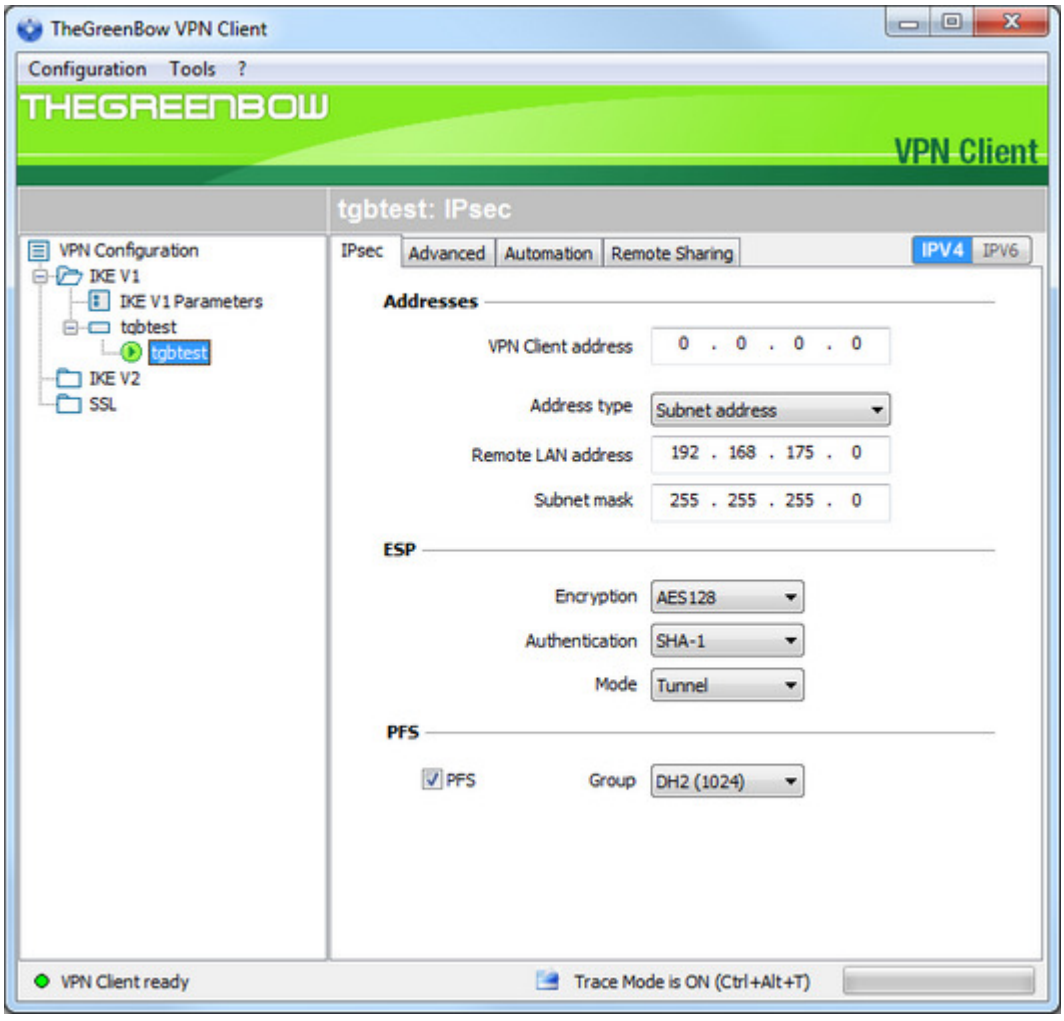
3.1 Opening a VPN tunnel

TheGreenBow VPN Client is provided with a VPN security policy for test: tgbtest
Launch the VPN Client and then use any of the following ways:

- in the taskbar, right click on the VPN Client icon, then click on "Open tgbtest-tgbtest"



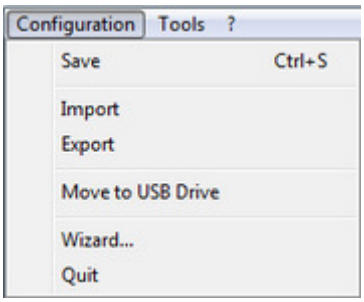
- in the Configuration Panel, double-click the "tgbtest" tunnel in the tree as shown below:



The VPN tunnel opens and TheGreenBow test website is automatically displayed.

3.2 Configuring a VPN tunnel

In the main interface, open the VPN Configuration Wizard: "Configuration" > "Wizard..."



Use the wizard as described in chapter "VPN Configuration Wizard".
To complete or refine the VPN configuration, you will find many configuration guides available for most VPN gateways on the TheGreenBow website: www.thegreenbow.com/vpn/vpn_gateway.html

3.3 Setting the automatic opening of a VPN tunnel

TheGreenBow VPN Client allows configuring a VPN tunnel so it opens automatically.

A VPN tunnel can be automatically opened:

1/ Upon detection of traffic to the remote network. See chapter "Automation"

2/ Upon opening (double-click) of a VPN security policy file (".tgb" file). See chapter "Automation"

3/ While inserting a USB drive containing the appropriate VPN security policy. See chapter "USB Mode"

4/ While inserting a token or a smartcard containing the certificate used for the tunnel. See chapter "Use a VPN Tunnel with a Certificate from a Smartcard"

4 User Interface

4.1 Overview

The VPN Client user interface allows to:
1/ configure the software itself (boot mode, language, access control, etc...)
2/ manage security policies (VPN configuration VPN tunnels, certificate management, import, export, etc...)
3/ use VPN tunnels (opening, closing, troubleshooting, etc...)

The user interface is divided into:
- The elements of the software available on the Windows Desktop (desktop icons, start menu)
- An Icon in Taskbar and its associated menu
- The Connection Panel (list of VPN tunnels to open)
- The Configuration Panel

The Configuration Panel is composed of the following elements:
- A set of Menus to manage the software and VPN security policies
- The VPN Tunnel tree
- Configuration tabs for VPN tunnels
- A Status bar

4.1.1 Windows Desktop

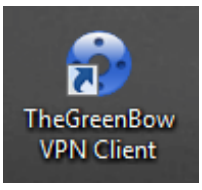
4.1.1.1 Startup Menu

After installation, the VPN Client can be launched from the Windows Start menu.

Two links are created in the directory TheGreenBow / TheGreenBow VPN start menu:
1/ Launch TheGreenBow VPN Client
2/ Uninstall TheGreenBow VPN Client

4.1.1.2 Desktop

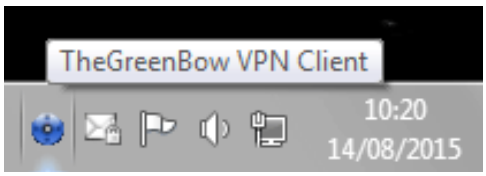
During the software installation, the application icon is created on the Windows desktop.
VPN Client can be launched directly by double-clicking on this icon.



4.2 Icon in Taskbar

4.2.1 Icon

In current usage, TheGreenBow VPN Client is identified by an icon located in the taskbar.



The icon color changes if the tunnel is open:

Blue icon: no VPN tunnel is open

Green icon: at least one VPN tunnel is open

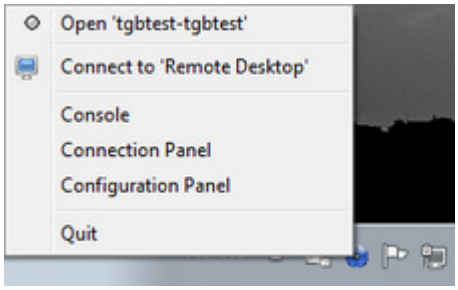
The "tooltip" the VPN Client icon indicates the status at any time of the software:
- "Tunnel <TunnelName>" if one or more tunnels are open.
- "Waiting VPN ready..." when VPN IKE is starting.
- "TheGreenBow VPN Client" when the VPN Client is launched without tunnel opened.

Left-click on the icon opens the software interface (Configuration Panel or Connection Panel).

Right-clicking the icon displays the menu associated with the icon.

4.2.2 Menu

Right click on the VPN Client icon in the taskbar displays the contextual menu associated with the icon:



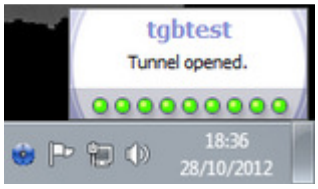
The contextual menu items are:

1/	List of VPN tunnels configured:	Click on the VPN tunnel to open or close
2/	List of remote desktop sharing sessions:	Click on a session to open or close
3/	Console:	Opens the VPN logs window
4/	Connection Panel:	Opens the Connection Panel
5/	Configuration Panel:	Open the Configuration Panel
6/	Quit:	Closes the open VPN tunnels and quit the software.

4.2.3 Taskbar popup

When opening or closing a VPN tunnel, a sliding popup window appears above the icon in the VPN taskbar. This window identifies the status of the tunnel during its opening or closing, and disappears automatically, unless the mouse is over:

Tunnel open



Tunnel close

Problem opening of the tunnel: the window displays brief explanation of the incident, and a clickable link to more information on this incident.

Note: The display of the popup window can be disabled in the menu "Tools" > "Options" > "View" tab, option "Don't show the systray sliding popup".

4.3 Connection Panel

Connection Panel list of VPN tunnels configured and can open or close them:

To open a VPN tunnel in Connection Panel: double-click on the VPN tunnel.

The icon to the left of the tunnel indicates its status:
- Closed tunnel
- Tunnel being opened
- Open tunnel
- Incident opening or closure of the tunnel

There is a gauge before each open tunnel that indicates in real time the volume of traffic exchanged in the tunnel.

The [?], [+] And [x] enables the following actions:
- [?]: Displays the "About..."
- [+]: Open the Configuration Panel
- [X] Close window

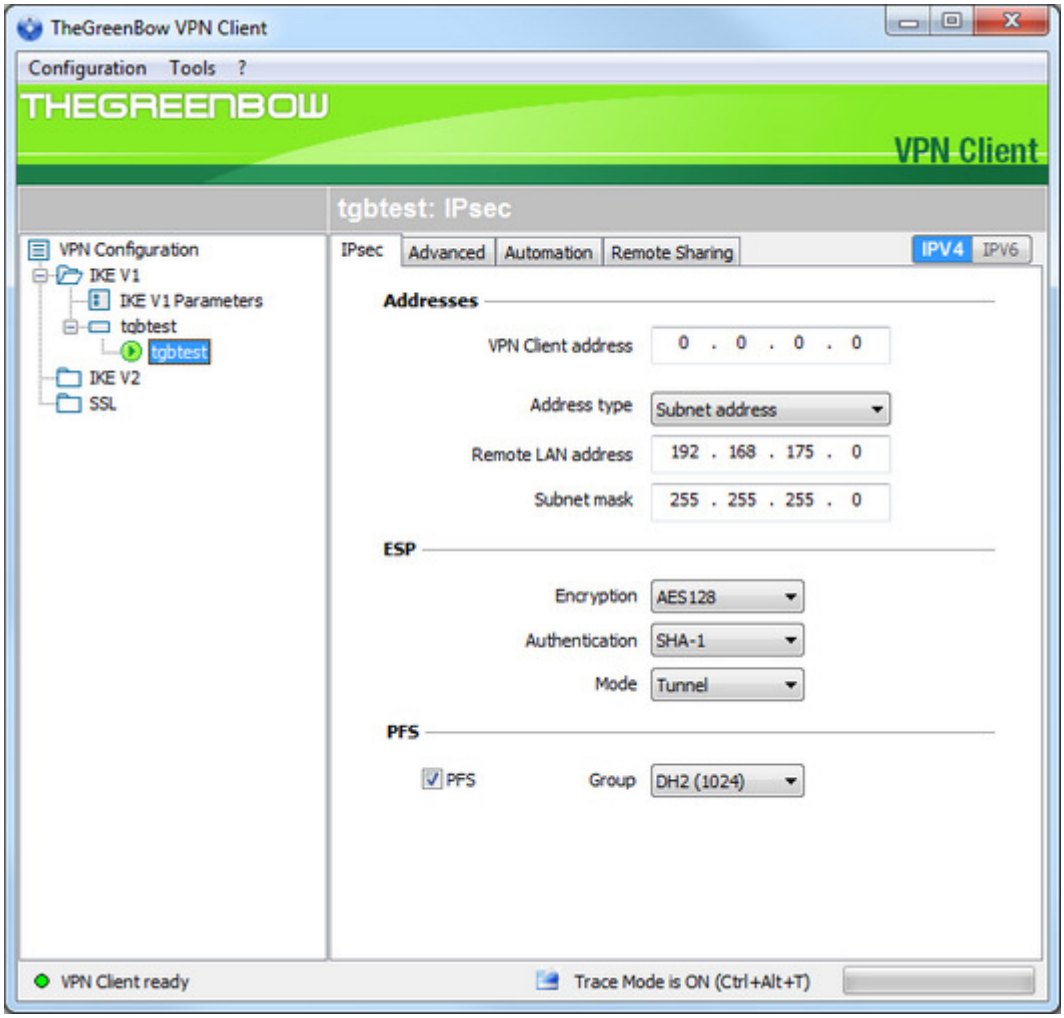
On the Connection Panel, the following shortcuts are available:
- ESC closes the window
- Ctrl+Enter opens the Configuration Panel

Note: Access to the Configuration Panel can be protected by a password. See chapter "Access control to the VPN security policy".

4.4 Configuration Panel

The Configuration Panel is composed of the following elements:

- A set of menus for managing software and VPN security policies
- The VPN tunnel tree
- Configuration tabs for VPN tunnels
- A status bar



4.4.1 Menus

The Configuration Panel menus are:

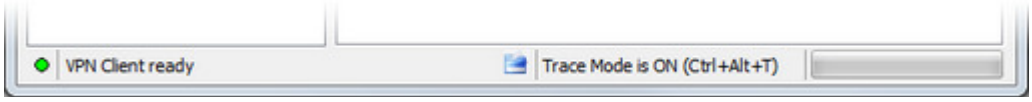
- "Configuration"
  - Import: Importing a VPN security policy (VPN Configuration)
  - Export: Exporting a VPN security policy (VPN Configuration)
  - Move to USB drive: USB Mode settings and enable the USB mode
  - VPN Configuration Wizard: **C**reating a VPN security policy
  - Quit: Close the open VPN tunnels and quit the software

- "Tools"
  - Connection Panel
  - Console: IKE connection trace Window
  - Reset IKE: Reboot IKE
  - Options: Options to restrict the display of some features, startup mode, language management

- "?"
  - Online Support: Access to online support
  - Software update: Check the availability of an update
  - Buy a license online: Access to the online shop
  - Activation Wizard
  - "About..." window

4.4.2 Status bar

The status bar at the bottom of the Configuration Panel provides more information:



- The "LED" on the far left is green when all services are operational software (IKE).
- The text to the left indicates the status of the software ("VPN ready", "Save configuration", "Apply Settings", etc...)
- When enabled, tracing mode is identified in the middle of the status bar. The icon "folder" on the left blue is a clickable icon that opens the folder containing the log files generated by the mode tracing.
- The progress bar on the right of the status bar identifies the progress of the backup of Configuration.

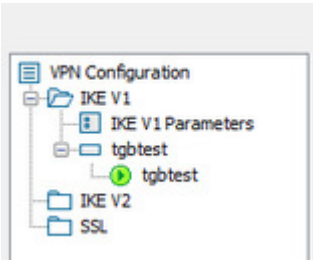
4.4.3 Shortcuts

Ctrl+Enter	Toggles the Connection Panel
Ctrl+D	Opens the "Console" VPN traces
Ctrl+Alt+R	Restart IKE
Ctrl+Alt+T	Trace mode activation (generation of logs). Works also with CTRL+Alt+D

4.4.4 VPN Tunnel tree

4.4.4.1 Introduction

The left side of the Configuration Panel is the tree representation of the VPN security policies. The tree can contain an unlimited number of VPN tunnels.



There are three entries at the root level which allow you to see, edit or create either:
1. IPsec tunnel using IKEv1 with multiple Phase 1 and Phase 2. Each Phase 1 can contain multiple Phase 2.
2. IPsec tunnel using IKEv2 with multiple IKE Auth and Child SA connections. Each IKE Auth can contain multiple Child SA.
3. SSL tunnel with multiple TLS connections.

1. IPsec IKEv1 VPN tunnel
- Clicking on a Phase 1 opens the configuration tabs for Phase 1 ("Configure IPsec IKEv1: Authentication").
- Clicking on a Phase 2 opens the configuration tabs for Phase 2 ("Configure IPsec IKEv1: IPsec").

2. IPsec IKEv2 VPN tunnel
- Clicking on a IKE Auth opens the configuration tabs for IKE Auth ("Configure IPsec IKev2: IKE Authentication").
- Clicking on a Child SA opens the configuration tabs for Child SA ("Configure IPsec IKEv2: Child SA").

3. SSL VPN tunnel
- Clicking on a TLS opens the configuration tabs for TLS ("Configure SSL: TLS connection").

The icon to the left of the tunnel indicates its status:
- Closed tunnel. Double-click on a this icon opens or closes the related VPN tunnel.
- Tunnel configured to automatically open on traffic detection
- Tunnel being opened
- Open tunnel
- Incident opening or closure of the tunnel

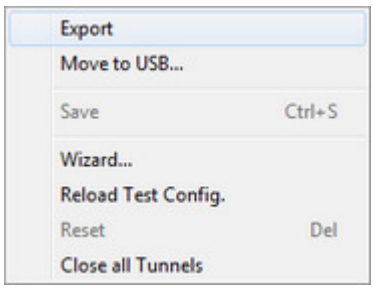
By clicking twice (slowly) on any item, it is possible to edit and modify the name of this item.

Note: Two items with the same root shall not have the same name. If the user enters a name that is already assigned, the software displays a warning.

Unsaved changes to the VPN Configuration are identified by bold font for the tunnel that changed. The tree returns to normal font when it is saved.

4.4.4.2 Contextual Menus

Right click on the VPN Configuration (root of the tree) displays the following context menu:



- Export — Exports the entire VPN security policy.
- Move USB... — Configure a USB flash drive to move in "USB Mode".
- Save — Saves the VPN security policy.
- Configuration Wizard — Opens the VPN Configuration Wizard
- Reload the default configuration — TheGreenBow VPN Client is installed with a default configuration that

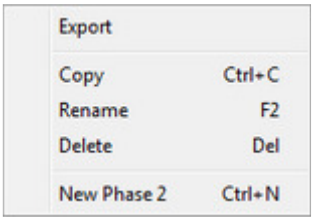
allows to test opening a VPN tunnel. This menu allows you to reload it at any time.

- Reset — Reset the VPN security policy, subject to confirmation by the user.
- Close all tunnels — Close all open tunnels.

1. IPsec with IKEv1 or IKEv2 VPN tunnel

Right click on an IKEv1 or IKEv2 displays the following contextual menu, and allows to create multiple Phase1 or IKE Auth:

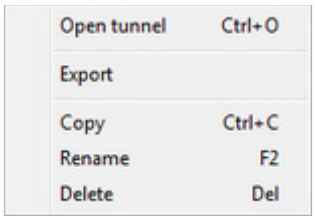
Right click on a Phase1 or IKE Auth displays the following contextual menu:



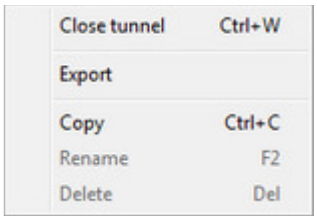
- Export — Exports the selected Phase1 or IKE Auth.
- Copy — Copies the selected Phase 1 or IKE Auth in the "clipboard".
- Rename (1) — Allows you to rename the selected Phase 1 or IKE Auth.
- Delete (1) — Delete, the entire Phase 1 or or IKE Auth, including all possible Phases 2 or Child SA associated with it. This is subject to confirmation by the user.
- New Phase 2 or Child SA — Adds a new Phase 2 to the selected Phase 1, or a new Child SA to the selected IKE Auth.

(1) This menu is disabled as long as a tunnel is open.

Right click on a Phase 2 or Child SA displays the following contextual menu:



Menu tunnel close



Menu tunnel open

- Open Tunnel — Displayed if the VPN tunnel is closed, opens the selected VPN tunnel.
- Close the tunnel — Displayed if the VPN tunnel is opened, to close the selected VPN tunnel.
- Export (1) — Exports the selected tunnel.
- Copy — Copies the selected tunnel.
- Rename (2) — Allows you to rename the selected tunnel.
- Delete (2) — Delete, subject to confirmation by the user, the selected tunnel.

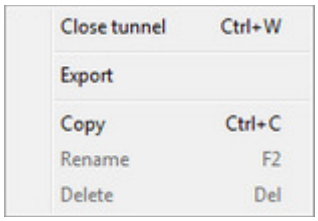
(1) This feature allows you to export the entire tunnel (i.e. the associated Phase 2-Phase 1 or IKE Auth-Child SA) and to create a single VPN tunnel security policy fully operational (which can for example be imported and immediately functional).
(2) This menu is disabled until the tunnel is open.

2. SSL VPN tunnel

Right click on SSL displays the following contextual menu, and allows to create multiple TLS connections:

Right click on a TLS connection displays the following contextual menu:

Menu tunnel close



Menu tunnel open

- Open Tunnel — Displayed if the SSL VPN tunnel is closed, opens the selected SSL VPN tunnel.
- Close the tunnel — Displayed if the SSL VPN tunnel is opened, to close the selected SSL VPN tunnel.
- Export (1) — Exports the selected tunnel.
- Copy — Copies the selected tunnel.
- Rename (2) — Allows you to rename the selected SSL tunnel.
- Delete (2) — Delete, subject to confirmation by the user, the selected SSL tunnel.

(1) This feature allows you to export the entire tunnel (i.e. TLS connection) and to create a single VPN tunnel security policy fully operational (which can for example be imported and immediately functional).
(2) This menu is disabled until the tunnel is open.

4.4.4.3 Shortcuts

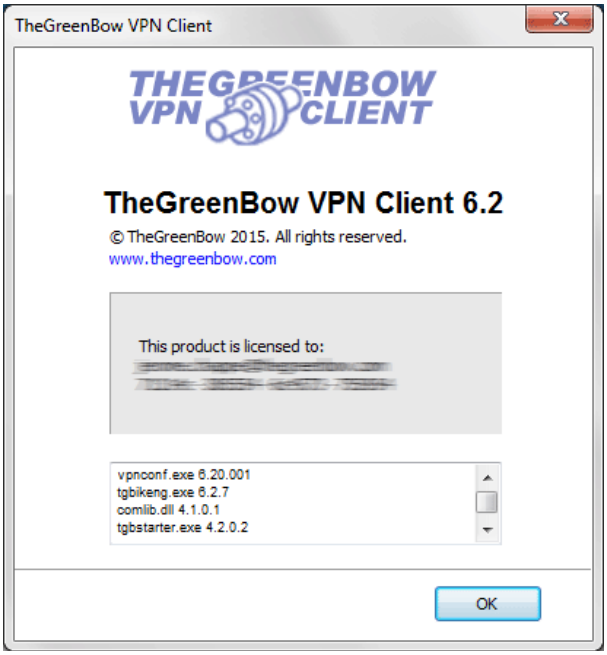
For the management of the tree, the following shortcuts are available:

- F2: Allows you to edit the name of the selected item
- DEL: If an item is selected, deletes after user confirmation.
  If the configuration is selected (root of the tree), moved the delete (reset) of the complete configuration.
- Ctrl+O: If a tunnel is selected, opens the corresponding VPN tunnel.
- Ctrl+W: If a tunnel is selected, closes the corresponding VPN tunnel.
- Ctrl+C: Copy the selected item in the "clipboard".
- Ctrl+V: Paste (adds) the copied item to the "clipboard".
- Ctrl+N: Creates a new item (e.g. Phase 1, Phase 2, IKE Auth, Child SA,...), if the VPN Configuration is selected.
- Ctrl+S: Save the VPN security policy.

4.4.5 "About" window

The "About..." is available via:

- the menu "Help" > "About..." from the Configuration Panel,
- the system menu in the Configuration Panel,
- or via the [?] of the Connection Panel.



The "About..." provides the following information:

- The name and version of the software.
- Internet link to the TheGreenBow website.
- When the software is activated, the license number and the email used for activation.
- When the software is in evaluation period, the number of days remaining in the evaluation.
- The versions of all software components (1).

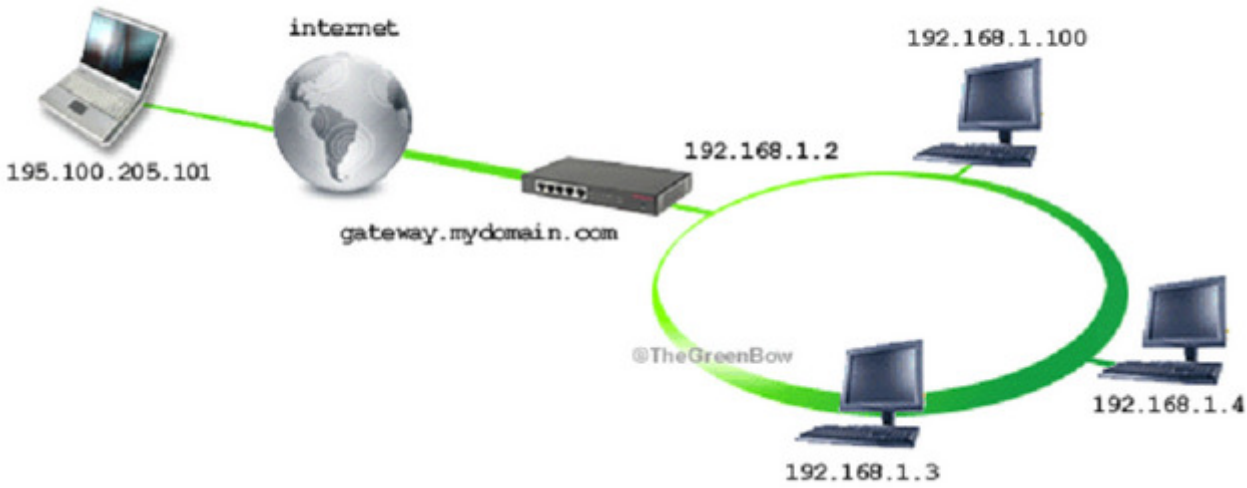
(1) It is possible to select all the contents of the list of versions (right click in the list and choose "Select All"), then copy it. It can be useful for debug purposes.

4.5 VPN Configuration Wizard

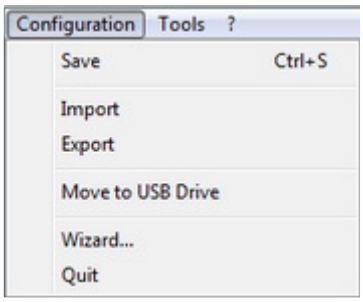
TheGreenBow VPN Client configuration wizard allows you to configure a VPN tunnel in 3 easy steps.

Using the Configuration Wizard is illustrated by the following example:

- The tunnel is opened between a computer and a VPN gateway with DNS address like "gateway.mydomain.com"
- The company's local network is 192.168.1.0 (it contains several machines with IP address such as 192.168.1.3, 192.168.1.4, etc...)
- Once the tunnel is open, the remote IP address in the corporate network will be: 192.168.1.50

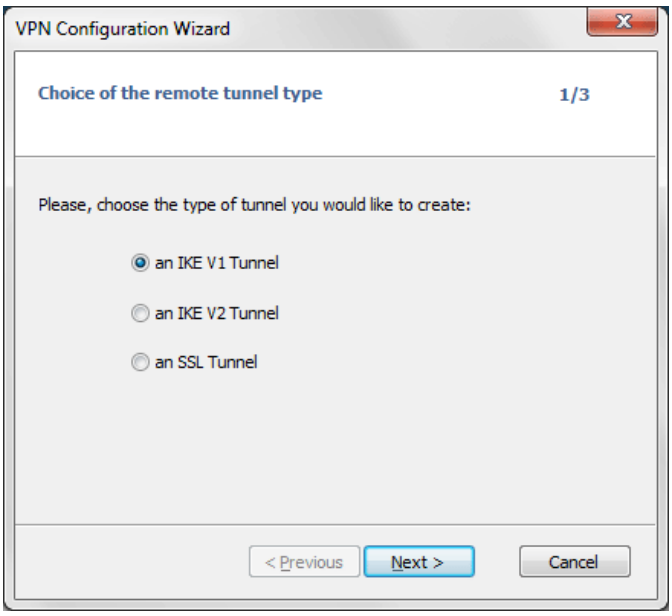


In the main interface, open the VPN Configuration Wizard: "Configuration" > " Wizard...".



Step1:

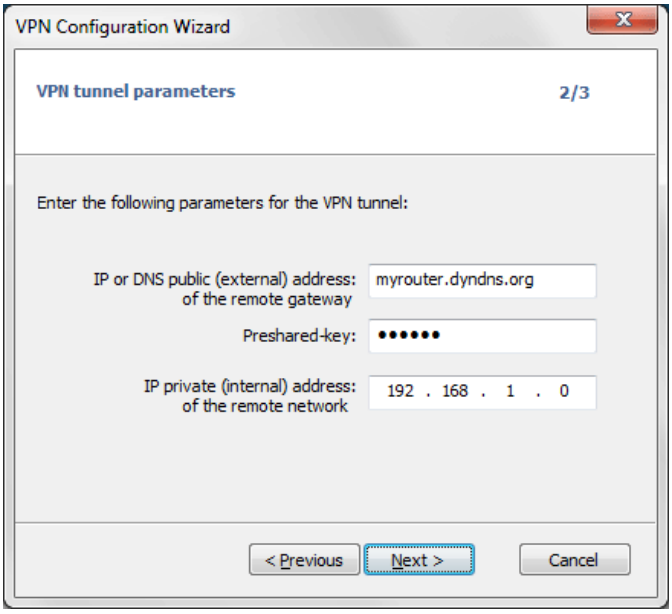
Choose the VPN protocol you want to use for the tunnel: IKE V1, IKE V2 or SSL.



Step2 with IKEv1 VPN:

Enter the following values:

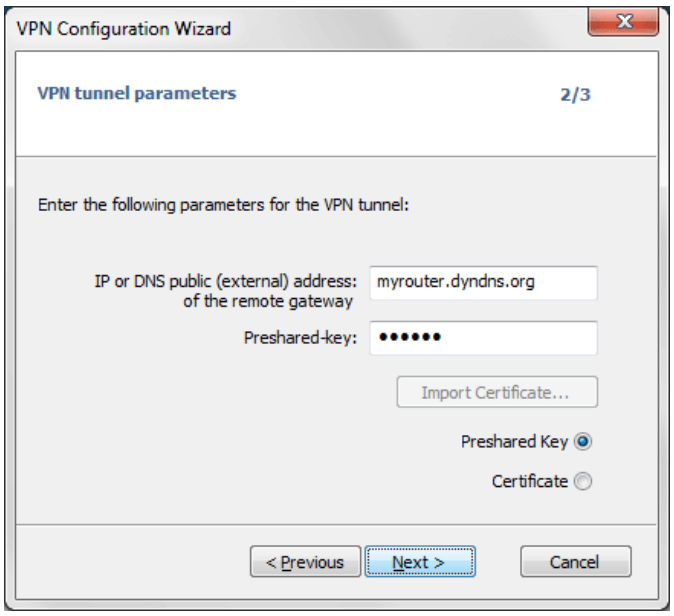
- The IP or DNS address of the VPN gateway on the Internet Network side (example: myrouuter.dyndns.org)
- A preshared key which must be the same on the VPN gateway
- The IP address of the network (LAN) of the company (example: 192.168.1.0)

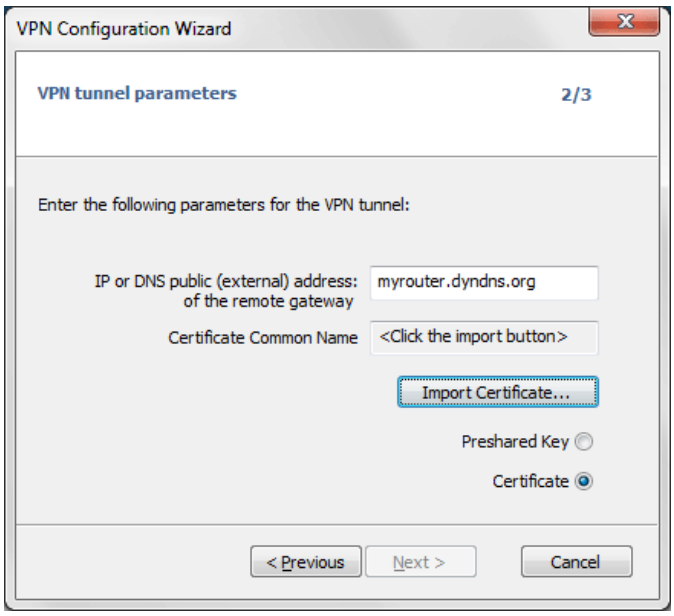


Step2 with IKEv2 VPN:

Enter the following values:

- The IP or DNS address of the VPN gateway on the Internet Network side (example: myrouuter.dyndns.org)
- A preshared key which must be the same on the VPN gateway or
- A Certificate which must be imported via the "Import Certificate..." button (see chapter "Import a certificate")

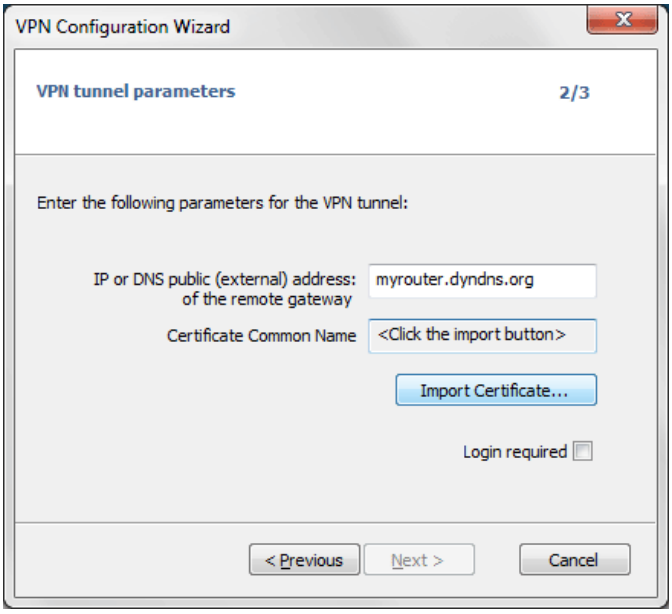




Step2 with SSL (OpenVPN) VPN:

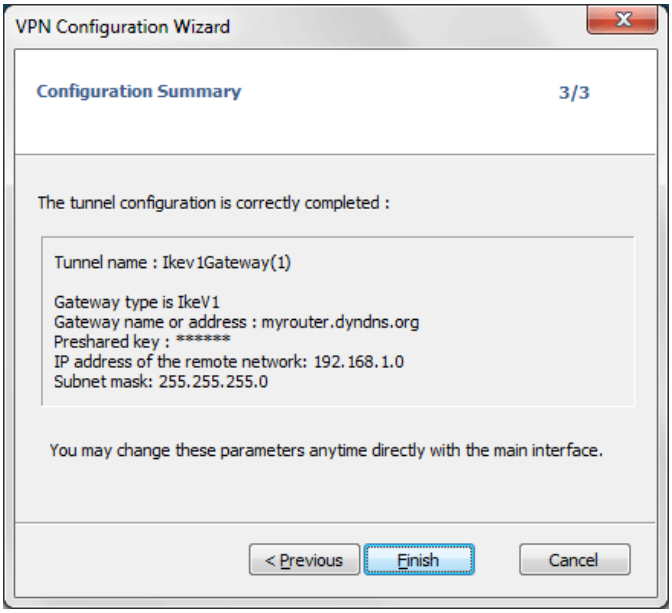
Enter the following values:

- The IP or DNS address of the VPN gateway on the Internet Network side (example: myrouuter.dyndns.org)
- A Certificate which must be imported via the "Import Certificate..." button (see chapter "Import a certificate")



Step3:

Check in the summary window that the settings are correct and click "FInish".
Example below for an IKEv1 VPN:



The VPN tunnelthat has been configured appears in the VPN tree of the Configuration Panel.
Double-click to open the tunnel or refine the configuration using the tabs in the Configuration Panel.

For more complex configuration or for additional information on how to configure VPN gateways, visit our website:
www.thegreenbow.com/vpn/vpn_gateway.html

5 Configure a VPN tunnel

5.1 Create a VPN tunnel

The VPN Client allows to create multiple VPN tunnels using multiple technologies. You can create a VPN tunnel:

- using IPsec with IKEv1
- using IPsec with IKEv2
- using SSL

Please have also a look at the navigation described in chapter "VPN Tunnel tree".

5.2 Save modifications

Save your configuration at any time using:

- Ctrl+S
- or menu "Configuration" then "Save".

5.3 Configure an IPsec VPN tunnel with IKEv1

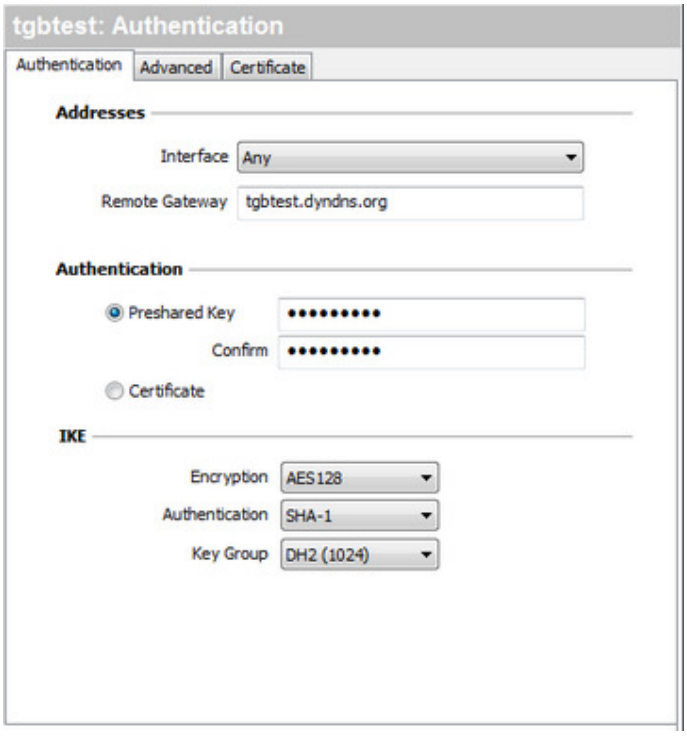
5.3.1 Configure Phase 1: Authentication

A VPN tunnel Phase 1 is the Authentication Phase in IKEv1.
Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of Phase 1, each end system must identify and authenticate itself to the other.

To configure Phase 1, select this Phase 1 in Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

Once setup is complete, you need to "save" for this configuration to be taken into account by the VPN Client.

5.3.1.1 Authentication



Interface	IP address of the network interface of the computer, through which VPN connection is established. The VPN Client can choose this interface if you select "Any". This is useful if you are configuring a tunnel that going to be used on other computer.
Remote Gateway	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). This field is mandatory.
Pre Shared Key	Password or key shared with the remote gateway. Note: The pre shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates. See "Recommendations for Security".
Certificates	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...). See chapter "Recommendations for Security". See chapter "Managing Certificates".
IKE - Encryption	Encryption algorithm used during Authentication phase: Auto (1), DES, 3DES, AES-128, AES-192, AES-256.
IKE - Authentication	Authentication algorithm used during Authentication phase: Auto (1), MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512.
IKE – Key Group	Diffie-Hellman key length DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)
IPv4 - IPv6	See chapter "IPv4 and IPv6 ready".

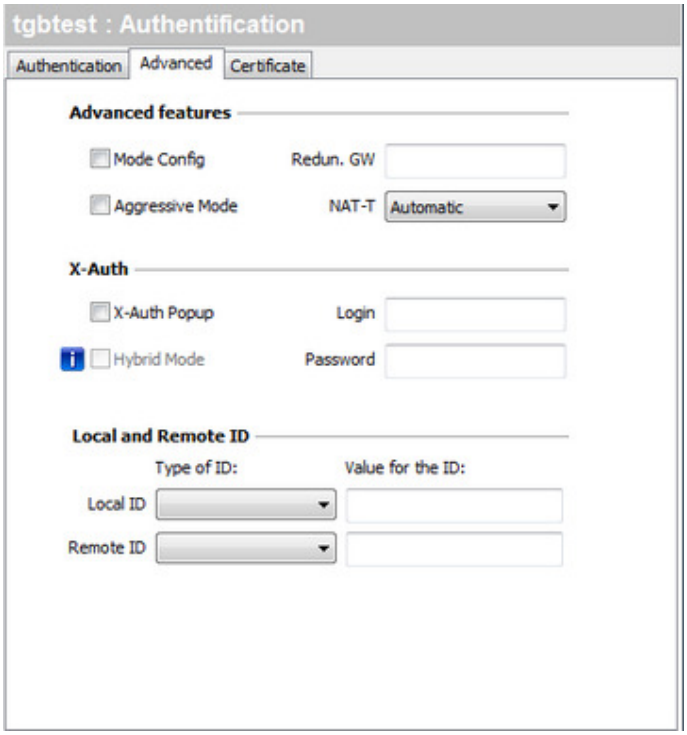
(1) Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When Auto is selected, the following algorithms (and their combinations) are supported:

- Encryption: 3DES, AES-128, AES-192
- Authentication: SHA-1, SHA2-256

- Key Group: DH1, DH2, DH5

If the gateway is configured with a different algorithm then Auto can't be used, and the algorithm must be explicitly specified in the VPN Client.

5.3.1.2 Authentication Advanced



Mode Config	If checked, the VPN Client will activate Config-Mode for this tunnel. Config-Mode allows to the VPN Client to fetch some VPN Configuration information from the VPN gateway. See "Mode Config" settings below.
Redundant Gateway	This allows the VPN Client to open an IPsec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com). See section "Managing Redundant Gateway" below.
Aggressive Mode	If checked, the VPN Client will used aggressive mode as negotiation mode with the remote gateway. See "Recommendations for Security" on Aggressive Mode vs. Main Mode.
NAT-T	The NAT-T mode allows Forced, Disabled and Automatic. "Disabled" prevents the VPN Client and the VPN gateway to start NAT-Traversal. "Automatic" mode leaves the VPN Gateway and VPN Client negotiate the NAT-Traversal. "Forced" mode, the VPN Client will force NAT-T by encapsulating IPsec packets into UDP frames to solve traversal with intermediate NAT routers.
X-Auth	See "Managing X-Auth" section below.

Hybrid Mode	Hybrid Mode is a mode that "blends" two types of authentication: classic VPN Gateway Authentication and X-Auth Authentication for VPN Client. To activate the Mode Hybrid, it is necessary that the tunnel is associated with a certificate (see "Managing Certificates"), and the X-Auth must be set. (See "Managing X-Auth" section below).
Local ID	"Local ID" is the identifier of the Authentication phase (Phase 1) that the VPN Client sends to the remote VPN gateway. Depending on the type selected, this identifier can be: - IP address (type = IP address), e.g. 195100205101 - A domain name (type = FQDN), e.g. gw.mydomain.net - Address (type = USER FQDN), e.g. support@thegreenbow.com - A string (type = KEY ID), e.g. 123456 - The subject of a certificate (type = Subject X509 (aka DER ASN1 DN)). This happens when the tunnel is associated with a user certificate (see "Managing Certificates"). When this parameter is not set, the IP address of the VPN Client is used by default.
Remote ID	"Remote ID" is the identifier the VPN Client expects from the remote VPN gateway. Depending on the type selected, this identifier can be: - IP address (type = IP address), e.g. 80.2.3.4 - A domain name (type = FQDN), e.g. routeur.mondomaine.com - Address (type = USER FQDN), e.g. admin@mydomain.com - A string (type = KEY ID), e.g. 123456 - The subject of a certificate (type = DER ASN1 DN) When this parameter is not specified, the IP address of the VPN gateway is used by default.

"Mode Config"

Mode Config, when activated, allows the VPN Client to recover some parameters from the VPN gateway configuration needed to open the VPN tunnel:
- Virtual IP address of the VPN Client
- The address of a DNS server (optional)
- The address of a WINS server (optional)

Important: the VPN gateway must support the Mode Config.

When the Mode Config is not enabled, all 3 parameters "VPN Client address", "DNS Server" and "WINS Server" can be configured manually in the VPN Client (see "Phase 2 IPsec Advanced").

When the Mode Config is activated, all 3 parameters "VPN Client address", "DNS Server" and "WINS Server" are automatically filled during the opening of the VPN tunnel. Therefore they cannot be modified manually.

Managing "Redundant Gateway"

The redundant gateway algorithm is the following:

VPN Client contacts the original Gateway to open the VPN tunnel.
If the tunnel can only be opened after N retries (N: see chapter "Configure Global Parameters")

The VPN Client contacts Gateway redundant.

The same algorithm applies to the Redundant Gateway: If the redundant gateway is unavailable, the VPN Client attempts to open the VPN tunnel with the original Gateway.

Note: The VPN Client does not try to contact the redundant gateway if the original Gateway is available and there are troubles opening of the tunnel.

Note: The use of redundant gateway can be coupled with the implementation of DPD (Dead Peer Detection, see "Configure Global Parameters"). Thus, when the VPN Client detects, through the DPD, the original gateway is unavailable, it automatically switches to the redundant gateway.

Managing "X-Auth"

X-Auth is an extension of the IKE protocol (Internet Key Exchange).

X-Auth is used to force the user to enter a login and a password before the opening the VPN tunnel.

Note: This feature requires a corresponding configuration on the VPN gateway.
When the "X-Auth Popup" is selected, a window will ask the login and password to authenticate the user each time a VPN tunnel open (the window requesting the login and password has the name of the tunnel to avoid confusion).

Upon time out (configurable in "**Global Parameters**"), a warning message alerts the user to re-open the tunnel.

Upon incorrect login/password, a warning message alerts the user to re-open the tunnel.

VPN Client allows you to store the login and password in the X-Auth VPN security policy. This login and password are automatically sent to the VPN Gateway when the tunnel opens.

This eases the use and deployment of software. However, it is still less secure than the popup window that asks X-Auth login/password when the tunnel opens.

It is recommended to look at the chapter "Recommendations for Security".

5.3.1.3 Certificate

See chapter "Managing Certificates".

5.3.2 Configure Phase 2: IPsec

The purpose of Phase 2 is to negotiate the IPsec security parameters that are applied to the traffic going through tunnels negotiated during Phase 1.

To configure a Phase 2, select this Phase 2 in the Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

After modification, you need to "save" for the configuration to be taken into account by the VPN Client.

5.3.2.1 IPsec

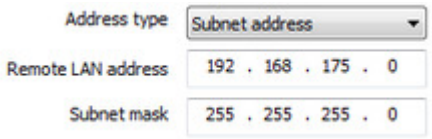
VPN Client address	This is the "virtual" IP address of the computer, as it will be "seen" on the remote network. Technically, it is the source IP address of IP packets carried in the IPsec tunnel. Note: If the Mode Config is enabled, this field is disabled. Indeed, it is automatically filled during the opening of the tunnel, with the value sent by the VPN gateway.
Address type	The remote endpoint may be a LAN or a single computer. See section "Address type configuration" below.
ESP - Encryption	Encryption algorithm negotiated during IPsec phase: Auto (1), DES, 3DES, AES-128, AES-192, AES-256.
ESP - Authentication	Authentication algorithm: Auto (1), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
ESP - Mode	IPsec encapsulation mode: tunnel or transport
PFS - Group	Diffie-Hellman key length if selected: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048)
IPv4-IPv6	See chapter "IPv4 and IPv6 ready".

(1) Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When Auto is selected, the following algorithms (and their combinations) are supported:
- Encryption: 3DES, AES-128, AES-192
- Authentication: SHA-1, SHA2-256

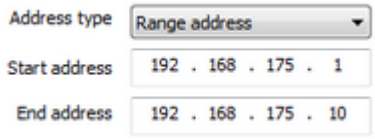
If the gateway is configured with a different algorithm then Auto can't be used, and the algorithm must be explicitly specified in the VPN Client.

"**Address type configuration**"

If the end of the tunnel is a network, choose the "Network Address" and then set the address and mask of the remote network:



Or choose "Range Address" and set the start address and the end address:



If the end of the tunnel is a computer, select "Single Address" and set the address of the remote computer:

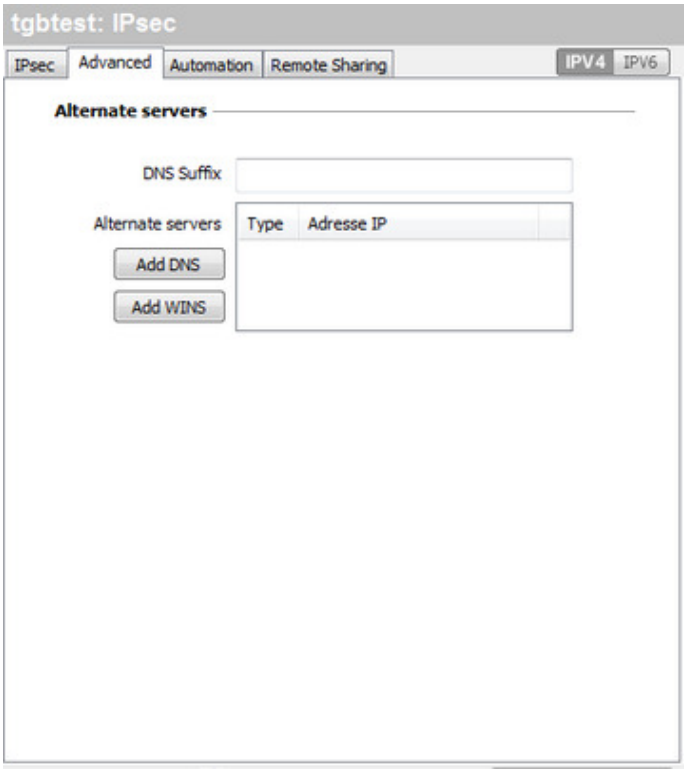
Note: The "Range Address" combined with the "Open automatically on traffic detection" allows to automatically open tunnel on traffic detection to one of the addresses in the specified address range (assuming the address range is also authorized in the configuration of the VPN gateway). "Open automatically on traffic detection" is also operational with the address type "subnet address" and "single address".

Note: If the IP address of the VPN Client is part of the IP address plan of the remote network (e.g. @IP poste = 192.168.10.2 and @remote network = 192.168.10.x), the opening of tunnel prevents the computer to contact its local network. All communications are routed within the VPN tunnel.

Configuration "all traffic through the VPN tunnel"
It is possible to configure the VPN Client to force all traffic exiting the computer passes through the VPN tunnel. To do so, select the address type "Network Address" and enter subnet mask as "0.0.0.0".

Reminder: Many configuration guides with different VPN Client VPN gateways are available on TheGreenBow website: www.thegreenbow.com/vpn/vpn_gateway.html.

5.3.2.2 IPsec Advanced



Alternate servers	− DNS suffix: Domain suffix to be added to any machine name e.g. mozart.dev.thegreenbow. Optional. The VPN Client will try to translate machine address without adding the DNS suffix. If the translation fails the VPN Client will add the DNS suffix and try to translate again. − Input field of IP addresses of DNS (2 max) and WINS (1 max) servers on the remote network. The IP address to be entered will be either IPv4 or IPv6 depending on the network selected in "IPsec" tab. Note: If the Mode Config is enabled, these fields are disabled. They are automatically filled in during the opening of the tunnel, with the values sent by the VPN gateway.

5.3.2.3 Automation

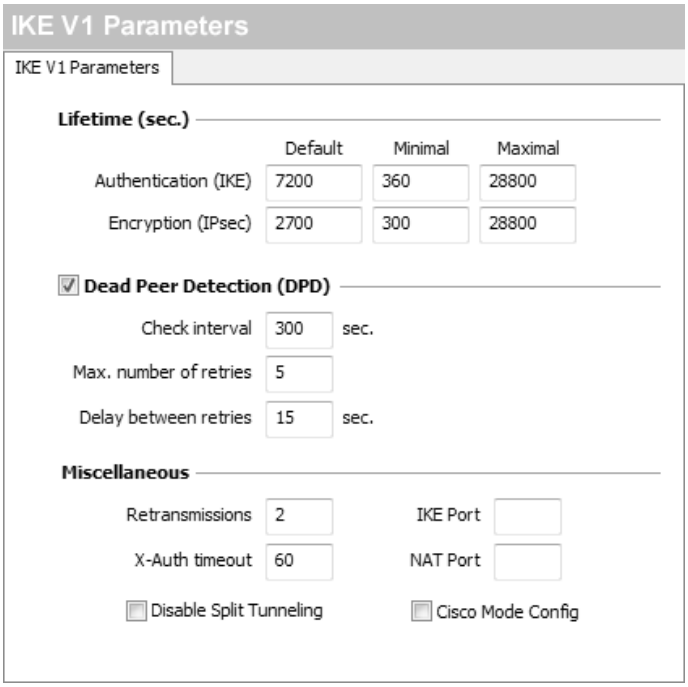
See chapter "Automation"

5.3.2.4 Remote Sharing

See chapter "Remote Desktop Sharing".

5.3.3 Configure IKEv1 Global Parameters

The IKEv1 global parameters are the parameters common to all VPN security policies using IKEv1 (all Phase 1 and Phase 2).
After modification, you need to "save" for the policy to be taken into account by the VPN Client.



Lifetime (sec.)	Lifetimes are negotiated when tunnel opens, between the VPN Client and the VPN gateway. Each peer is expected to transmit the "default" lifetime and to verify that the lifetime of the other peer is in the expected range (between minimal and maximal value). (1) When a lifetime expires (Phase 1 for Authentication or Phase 2 for encryption) the relevant phase is renegotiated. Lifetimes are expressed in seconds. The default values are:

	Default	Min	Max
Authentication (IKE)	7200 (2h)	360 (6min)	28800 (8h)
Encryption (IKE)	2700 (45min)	300 (5min)	28800 (8h)

DPD	DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive. (2) – Audit Period: Period between 2 DPD verification messages sent. – Number of attempts: Number of consecutive unsuccessful attempts before declaring the remote gateway unreachable – Time between attempts: Interval between DPD messages when no response is received from the VPN gateway.
Retransmissions	Number of IKE protocol messages retransmissions before failure.
X-Auth timeout	Time to enter the X-Auth login/password
Port IKE	IKE Phase 1 exchanges (Authentication) are performed on the UDP protocol, using the default port 500. Some network devices (firewalls, routers) filter port 500. Setting of the IKE port allows to get through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Phase 1 exchanges on a different port than 500.

Port NAT	IKE Phase 2 exchanges (IPsec) are performed on the UDP protocol, using default port 4500. Some network devices (firewalls, routers) filter port 4500. Setting of the IKE port allows to get through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Phase 2 exchange on a different port than 4500.
Disable Split Tunneling	When this option is checked, only the traffic through the tunnel is allowed. (3)

(1) Lifetimes are expected to be negotiated between the VPN Client and the VPN Gateway. However, some VPN Gateways just return the default lifetime value proposed by the VPN Client. In any case, the VPN Client always applies the lifetime sent by the VPN Gateway.

(2) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "Redundant Gateway", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

(3) The configuration option "Disable Split Tunneling" increases the security of the computer, when the VPN tunnel is opened. This feature prevents the risk of incoming traffic that could pass through the VPN tunnel. Associated with the configuration option "Force all traffic in the tunnel" (see chapter "IPsec"), this option ensures a complete sealing of the computer, as soon as the VPN tunnel is opened.

5.4 Configure an IPsec VPN tunnel with IKEv2

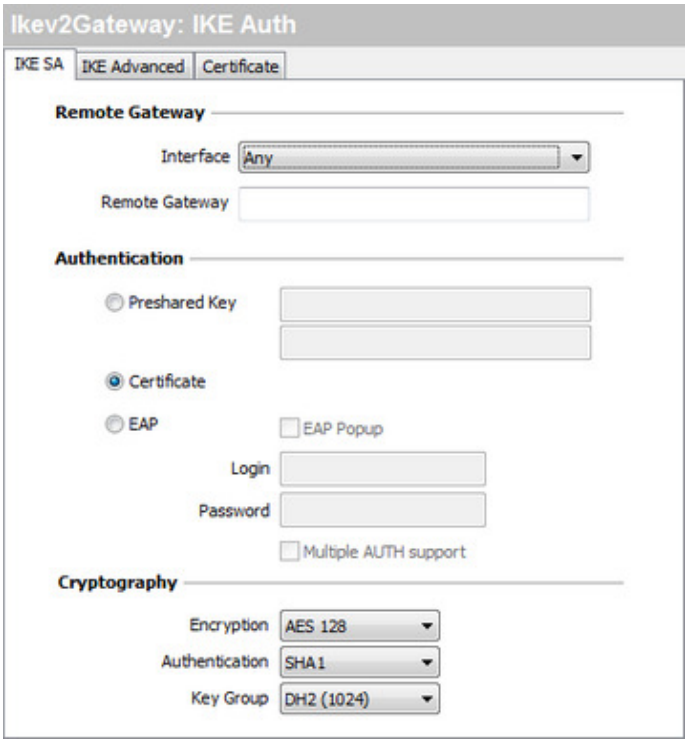
5.4.1 Configure IKE Auth

A VPN tunnel IKE Auth is the Authentication Phase in IKEv2.
IKE Auth's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of IKE Auth, each end system must identify and authenticate itself to the other.

To configure IKE Auth, select this IKE Auth in Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

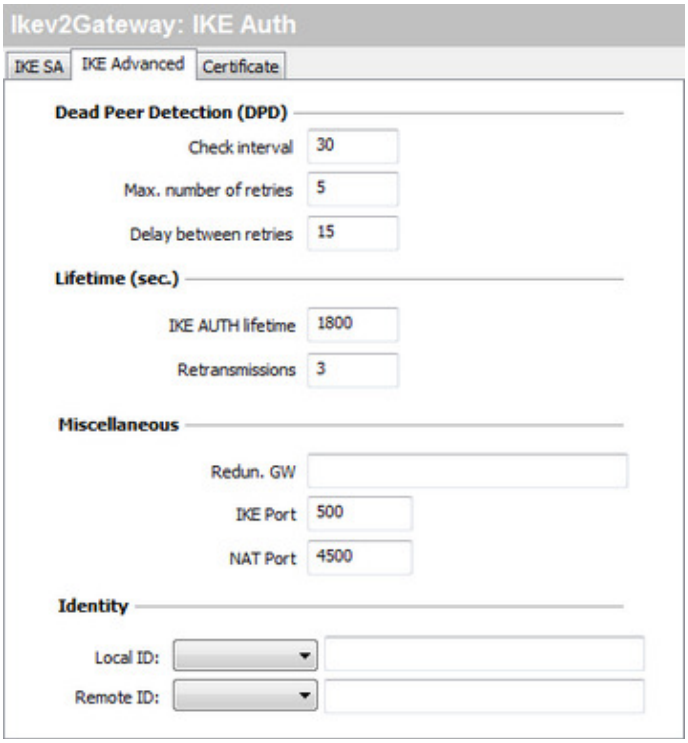
Once setup is complete, you need to "save" for this configuration to be taken into account by the VPN Client.

5.4.1.1 IKE SA



Interface	Name of the network interface of the computer, through which VPN connection is established. Selecting "Any" enables the VPN Client to automatically choose the appropriate interface.
Remote Gateway	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). This field is mandatory.
Authentication - Pre Shared Key	Password or key shared with the remote gateway. Note: The pre shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates. See "Recommendations for Security".
Authentication - Certificates	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...). See chapter "Recommendations for Security". See chapter "Managing Certificates".
Authentication - EAP	EAP (i.e. Extensible Authentication Protocol) enables to authenticate the user through a login/password. When the "EAP Popup" is selected, a window will ask the login and password to authenticate the user each time a VPN tunnel opens.
Multiple Auth Support	Multiple Auth Support enables the double authentication: Certificate then EAP. Note: The double authentication "EAP then certificate" is not supported by the VPN Client.
IKE - Encryption	Encryption algorithm used during Authentication phase: DES, 3DES, AES-128, AES-192, AES-256
IKE - Authentication	Authentication algorithm used during Authentication phase: MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
IKE - Key Group	Diffie-Hellman key length DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)

5.4.1.2 IKE Advanced



DPD	DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive. (1) - Audit Period: Period between 2 DPD verification messages sent. - Number of attempts: Number of consecutive unsuccessful attempts before declaring the remote gateway unreachable - Time between attempts: Interval between DPD messages when no response is received from the VPN gateway.
Retransmissions	Number of IKE protocol messages retransmissions before failure.
IKE Auth lifetime	Lifetimes of IKE Authentication phase. Expressed in seconds. Lifetimes are not negotiated during IKEv2 exchanges.
Redundant Gateway	This allows the VPN Client to open an IPsec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com). See section "Managing Redundant Gateway" below.
Port IKE	IKE Auth phase exchanges (Authentication) are performed on the UDP protocol, using the default port 500. Some network devices (firewalls, routers) filter port 500. Setting of the IKE port allows to get through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Auth Phase exchanges on a different port than 500.
Port NAT	Child SA phase exchanges (IPsec) are performed on the UDP protocol, using default port 4500. Some network devices (firewalls, routers) filter port 4500. Setting of the NAT port allows to get through these filtering devices. Note: The remote VPN gateway must also be capable of performing the Child SA phase exchange on a different port than 4500.

Local ID	"Local ID" is the identifier of the Authentication phase (IKE Auth) that the VPN Client sends to the remote VPN gateway. Depending on the type selected, this identifier can be: − IP address (type = IP address), e.g. 195100205101. Both IPv4 or IPv6 addresses are supported. − A domain name (type = FQDN), e.g. gw.mydomain.net − Address (type = USER FQDN), e.g. support@thegreenbow.com − A string (type = KEY ID), e.g. 123456 − The subject of a certificate (type = Subject X509 (aka DER ASN1 DN)). This happens when the tunnel is associated with a user certificate (see "Managing Certificates").
Remote ID	"Remote ID" is the identifier the VPN Client expects from the remote VPN gateway. Depending on the type selected, this identifier can be: − IP address (type = IP address), e.g. 80.2.3.4. Both IPv4 or IPv6 addresses are supported. − A domain name (type = FQDN), e.g. routeur.mondomaine.com − Address (type = USER FQDN), e.g. admin@mydomain.com − A string (type = KEY ID), e.g. 123456 − The subject of a certificate (type = DER ASN1 DN)

(1) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "**Redundant Gateway**", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

5.4.1.3 Certificate

See chapter "Managing Certificates".

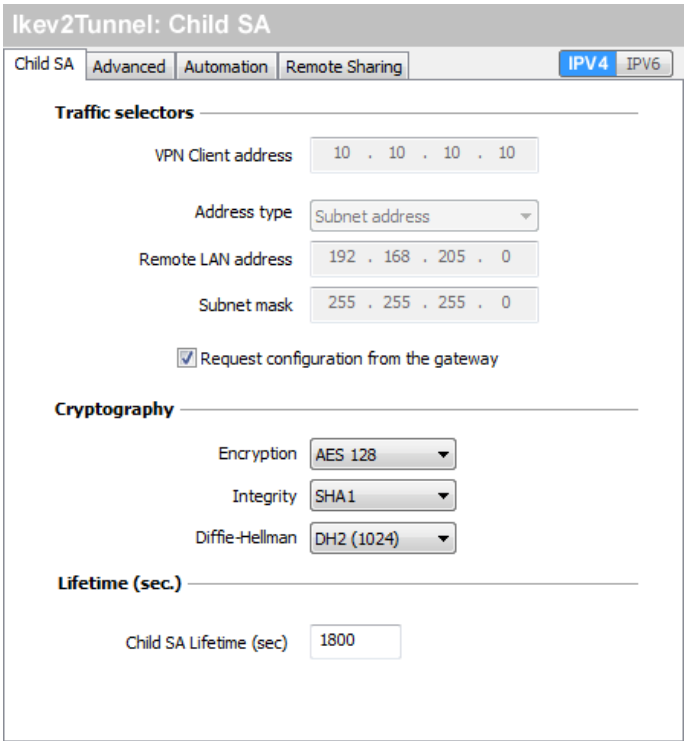
5.4.2 Configure Child SA

The purpose of Child SA is to negotiate the IPsec security parameters that are applied to the traffic going through tunnels negotiated during IKE Auth.

To configure a Child SA, select this Child SA in the Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

After modification, you need to "save" for the configuration to be taken into account by the VPN Client.

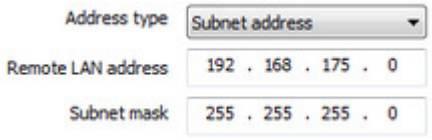
5.4.2.1 Child SA



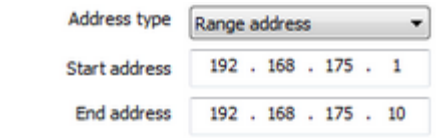
VPN Client address	This is the "virtual" IP address of the computer, as it will be "seen" on the remote network. Technically, it is the source IP address of IP packets carried in the IPsec tunnel. (1)
Address type	The remote endpoint may be a LAN or a single computer. See section "Address type configuration" below.
Remote LAN address - mask	The remote endpoint may be a LAN or a single computer. Set the address and mask of the remote network. (1)
Request configuration from the gateway	When this option is selected (also known as "Configuration Payload" or "CP"), all information (VPN Client address, Remote LAN address, Subnet mask and DNS adresses) are sent by the VPN gateway. Each field is grayed. It is filled in dynamically during the opening of the tunnel as soon as the values are received from the VPN gateway.
Cryptography - Encryption	Encryption algorithm negotiated during IPsec phase DES, 3DES, AES-128, AES-192, AES-256
Cryptography - Integrity	Authentication algorithm negotiated during IPsec phase MD5, SHA-1 and SHA-256 (i.e. SHA-2)
Cryptography - Diffie-Hellman	Diffie-Hellman key length if selected DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048)
Child SA lifetime	Child SA time in seconds before re-negotiation. Lifetimes are not negotiated during IKEv2 exchanges.
IPv4-IPv6	See chapter "IPv4 and IPv6 ready".

"**Address type configuration**"

If the end of the tunnel is a network, choose the "Network Address" and then set the address and mask of the remote network:



Or choose "Range Address" and set the start address and the end address:



If the end of the tunnel is a computer, select "Single Address" and set the address of the remote computer:

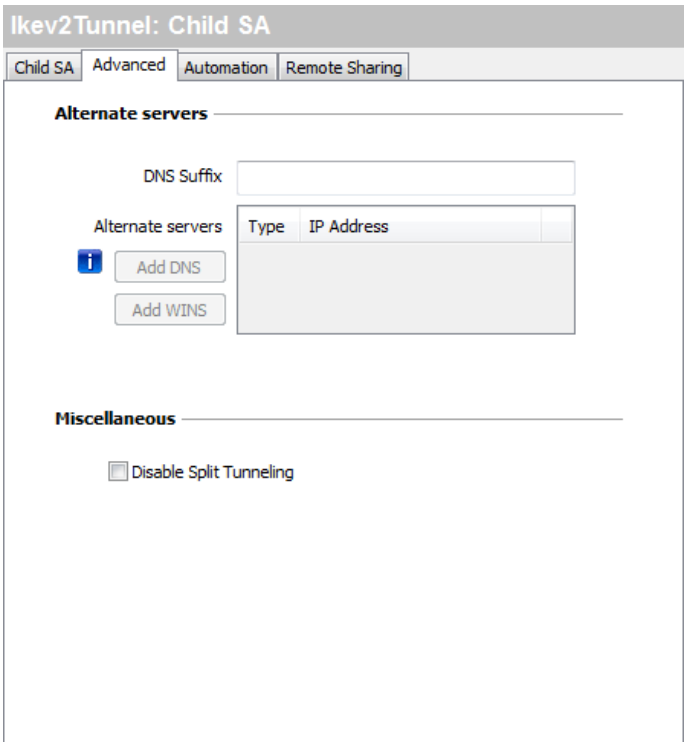
Note: The "Range Address" combined with the "Open automatically on traffic detection" allows to automatically open tunnel on traffic detection to one of the addresses in the specified address range (assuming the address range is also authorized in the configuration of the VPN gateway). "Open automatically on traffic detection" is also operational with the address type "subnet address" and "single address".

Note: If the IP address of the VPN Client is part of the IP address plan of the remote network (e.g. @IP poste = 192.168.10.2 and @remote network = 192.168.10.x), the opening of tunnel prevents the computer to contact its local network. All communications are routed within the VPN tunnel.

Configuration "all traffic through the VPN tunnel"
It is possible to configure the VPN Client to force all traffic exiting the computer passes through the VPN tunnel. To do so, select the address type "Network Address" and enter subnet mask as "0.0.0.0".

Reminder: Many configuration guides with different VPN Client VPN gateways are available on TheGreenBow website: www.thegreenbow.com/vpn/vpn_gateway.html.

5.4.2.2 Child SA Advanced



Alternate servers	DNS suffix: Domain suffix to be added to any machine name e.g. mozart.dev.thegreenbow. Optional. The VPN Client will try to translate machine address without adding the DNS suffix. if the translation fails the VPN Client will add the DNS suffix and try to translate again. – Input field of IP addresses of DNS (2 max) and WINS (1 max) servers on the remote network.The IP address to be entered will be either IPv4 or IPv6 depending on the network selected in "Child SA" tab. Note: If the "Configuration Payload" (a.k.a CP) is enabled, these fields are disabled. They are automatically filled in during the opening of the tunnel, with the values sent by the VPN gateway.
Disable Split tunneling	When this option is checked, only the traffic through the tunnel is allowed. (4)

(1) This option allows you to configure to open a tunnel automatically when double-click on the file ".tgb": Select the option "Automatically open this tunnel when the VPN Client starts," save and export the configuration file "tunnel_auto.tgb" leave the VPN Client. By double-clicking on the file "tunnel_auto.tgb" VPN Client starts and the tunnel opens automatically.

(2) By extension, this option is also used to configure a tunnel to open automatically when a Smartcard or a token containing the certificate used by the VPN tunnel is plugged in. See chapter "Use a VPN Tunnel with a Certificate from a SmarCard".

(3) Gina Credential Providers in Windows Vista, Windows 7 and further.

(4) The configuration option "Disable Split Tunneling" increasing security of the computer, when the VPN tunnel is opened. In particular, this feature prevents the risk of incoming traffic that could pass through the VPN tunnel. Associated with the configuration "Force all traffic in the tunnel" (see chapter "IPsec"), this option ensures complete sealing of the computer, when the VPN tunnel is opened.

5.4.2.3 Automation

See chapter "Automation"

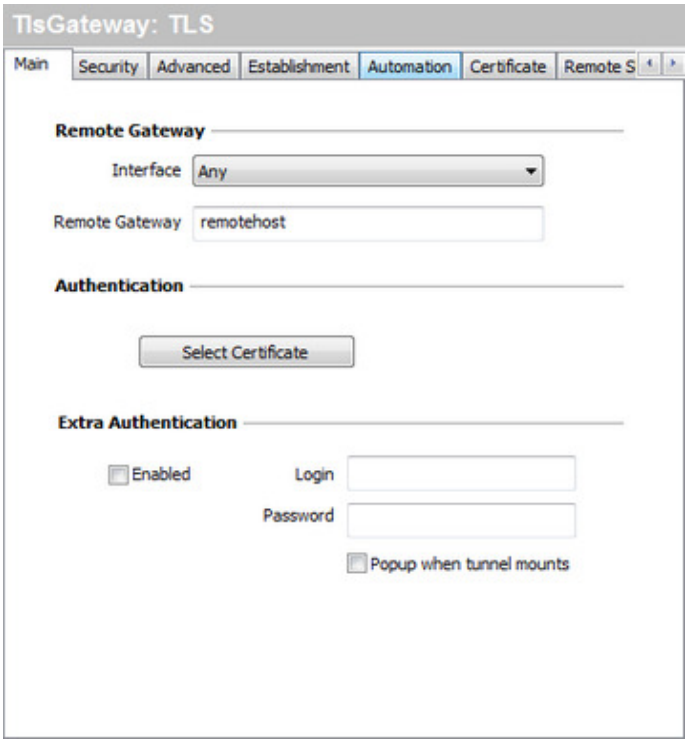
5.4.2.4 Remote Sharing

See chapter "Remote Desktop Sharing".

5.5 Configure a SSL VPN tunnel

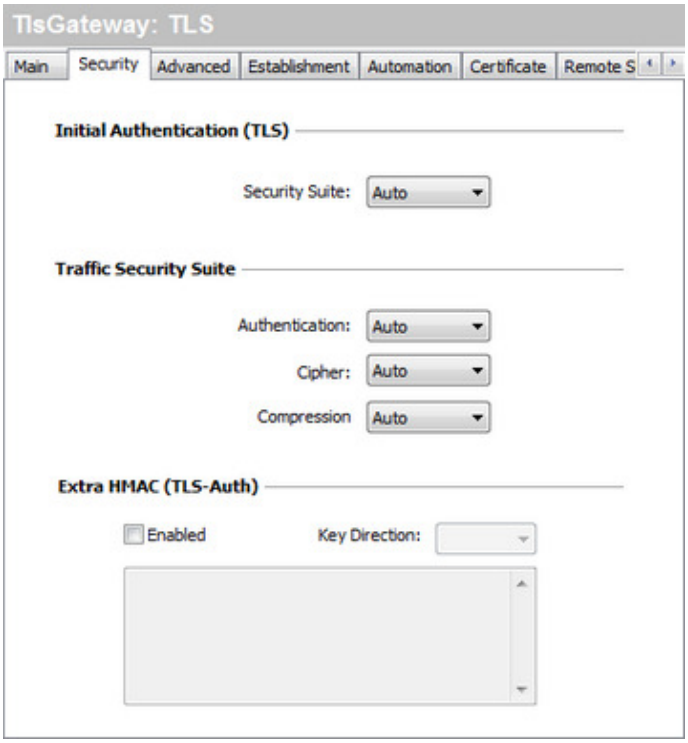
5.5.1 Configure a SSL VPN tunnel

5.5.1.1 Main parameters



Interface	Name of the network interface of the computer, through which VPN connection is established. Selecting "Any" enables the VPN Client to automatically choose the appropriate interface.
Remote Gateway	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). This field is mandatory.
Certificates	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...). See chapter "Recommendations for Security". See chapter "Managing Certificates".
Extra Authentication	Extra Authentication is an extra level of security that will request the user to enter a login and password to open the VPN tunnel. If enabled, the login and password can be entered here or in a popup if the option 'Popup when tunnel opens' is selected.

5.5.1.2 Security

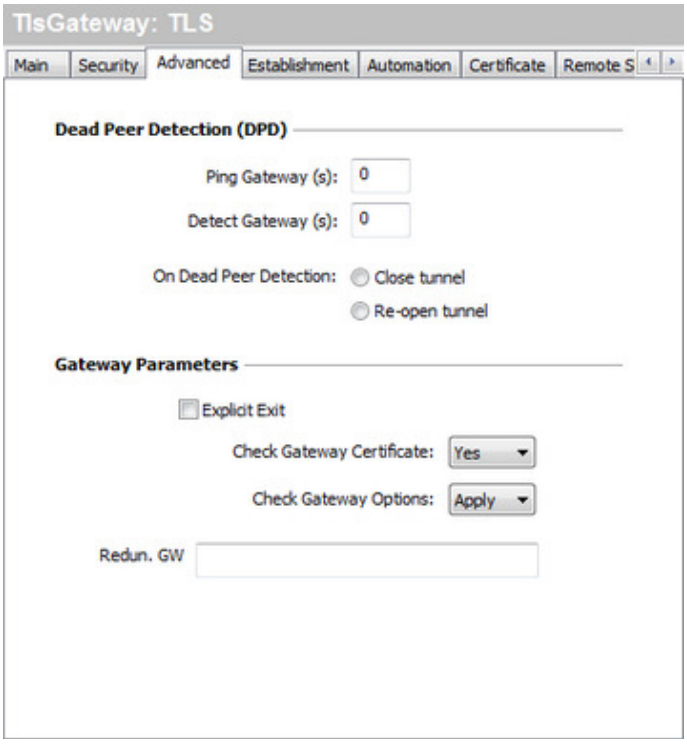


Authentication - Security Suite	It is used in the SSL handshake phase to authenticate both parties. It can be set to Auto (1), Low, Normal, High. Each items of this dropdown menu is a pre-selection of algorithms as follow: - Auto: All cipher suites except the null ciphers are proposed to the gateway. The gateway then decides the best security suite. - Low: Only 'low' encryption cipher suites are proposed to the gateway; currently, those using 64 or 56 bit encryption algorithms. - Normal: Only 'medium' encryption cipher suites are proposed to the gateway; currently, some of those using 128 bit encryption. - High: Only 'high' encryption cipher suites are proposed to the gateway; currently, those with key lengths larger than 128 bits, and some cipher suites with 128-bit keys. Reference for more information: https://www.openssl.org/docs/apps/ciphers.html
Traffic - Authentication	Authentication algorithm negotiated for the traffic Auto (1), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
Traffic - Cipher	Encryption algorithm of the traffic: Auto (1), BF-CBC-128, AES128-CBC, AES192-CBC, AES256-CBC.
Traffic - Compression	Compression of the traffic is optional and can be automatic as well (1).

Extra HMAC	This option adds an authentication level to packets exchanged between the client and the gateway. To be used on the client, the server has also to be configured with this option (on server the option is often called “TLS-Auth”). Selecting this option enables to enter a key in the text area below the checkbox. The "Key direction" must then be selected: Options are Auto (1), Bidirectionnal, Client or Server. The key must be the same as the one configured in the VPN gateway. The key direction "Client" must be set if the key direction of the VPN gateway is "Server", and conversely.

(1) Auto means that the VPN Client will adapt automatically to the settings of the gateway.

5.5.1.3 Advanced

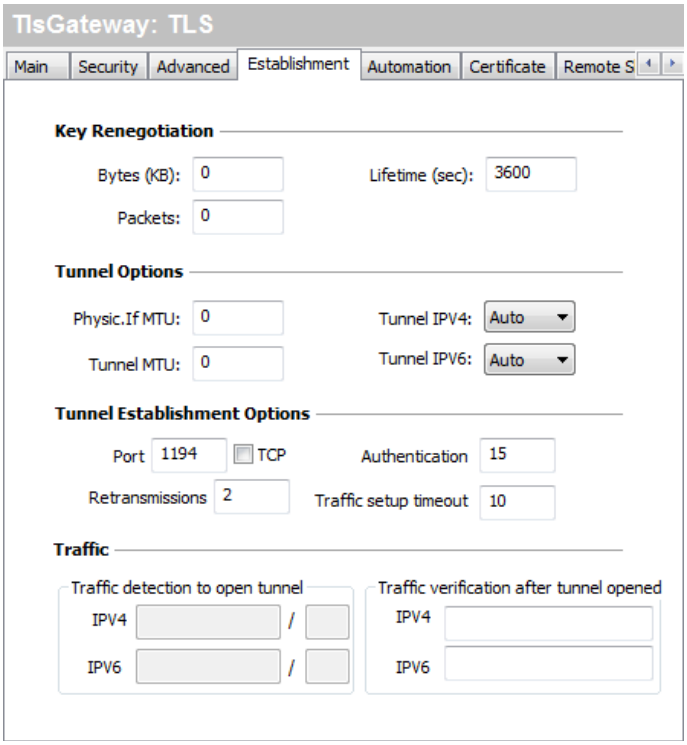


DPD	DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive, and reversely to allow the gateway to detect the client is no longer alive. (1) - Ping Gateway (seconds): Time in seconds between pings sent to the gateway. This is used by the gateway to know if the client is still there. - Detect Gateway (seconds): Timeout in seconds before considering the gateway dead because no ping was received from the gateway.
On Dead Peer Detection	Once the gateway has been detected to be dead (i.e. at the end of the timeout entered in "Detect gateway"), you can decide to close the VPN tunnel, or keep trying to re-open the VPN tunnel.

Gateway Parameters	Several parameters can be set: – Check Gateway Certificate with the following options: Yes, No, Lite. Level of control executed on the certificate received from the gateway. 'Yes' is full control of certificate validity, 'Lite' is for future use, and is not yet active in this release (same behavior as selecting 'Yes'). – Check Gateway Options with the following options: Yes, No, Lite, Apply. Level of control on coherency of settings (e.g. encryption algorithm, compression,..) between the VPN Client and the gateway. – 'Yes' means the VPN tunnel can not open if at least one setting differs from the gateway. – 'No' means no control on settings is done before opening VPN tunnel. The settings must be identical for the VPN tunnel to open. – 'Lite' means some control are done to check that there is coherency of settings with the gateway. – 'Apply' means the VPN Client will apply the settings sent by the gateway.
Redundant Gateway	This allows the VPN Client to open a tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com). See section "Managing Redundant Gateway" below.

(1) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "Redundant Gateway", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

5.5.1.4 Establishment



Key Renegotiation	– Lifetime (sec.): Time in seconds before a new Key negotiation shall occur. – Bytes (KB): Number of bytes before a new Key negotiation shall occur. Bytes is expressed in KB.

	- Packets: Number of packets before a new Key negotiation shall occur.
Tunnel Options	- Physic.If MTU: Maximum packet size on the physical network interface. Physic.If MTU is expressed in bytes. If 0, the MTU of the physical interface is not changed, it is used as configured by Windows. - Tunnel MTU: Maximum packet size on the virtual network interface. This is expressed in bytes.. If 0, the MTU of the virtual interface is computed automatically by the VPN Client. - Tunnel IPv4 with the following options: Auto (1), Yes, No. - Tunnel IPv6 with the following options: Auto (1), Yes, No.
Tunnel Establishment Options	- TCP: select the checkbox if the VPN gateway is configured in TCP mode. By default (and this is the standard) UDP is used. - Port: select the UDP (or TCP) port to be used to open the tunnel. Default is 1194. - Packet retries: Number of SSL protocol message retransmissions before failure. - Authentication timeout: TLS handshake timeout before giving up. - Traffic setup timeout: Traffic setup timeout before giving up.
Tunnel Establishment Options	- UDP port to be used to open the tunnel. Default is 1194. - Packet retries: Number of SSL protocol message retransmissions before failure. - Authentication timeout: TLS handshake timeout before giving up. - Traffic setup timeout: Traffic setup timeout before giving up.
Traffic - detection to open tunnel	If 'Auto open on traffic detection' is selected in the 'Automation' tab, enter here the network IP address that will be used to detect traffic to. Remote network can be either IPv4 or IPv6 or both in which case you must fill in both fields.
Traffic - verification after tunnel opened	Enter here a specific IP address on the remote network. Once VPN tunnel opened, a ping to this IP address is sent one time to check that traffic can go through. A message is displayed in the 'Console' if this fails.

5.5.1.5 Automation

See chapter "Automation"

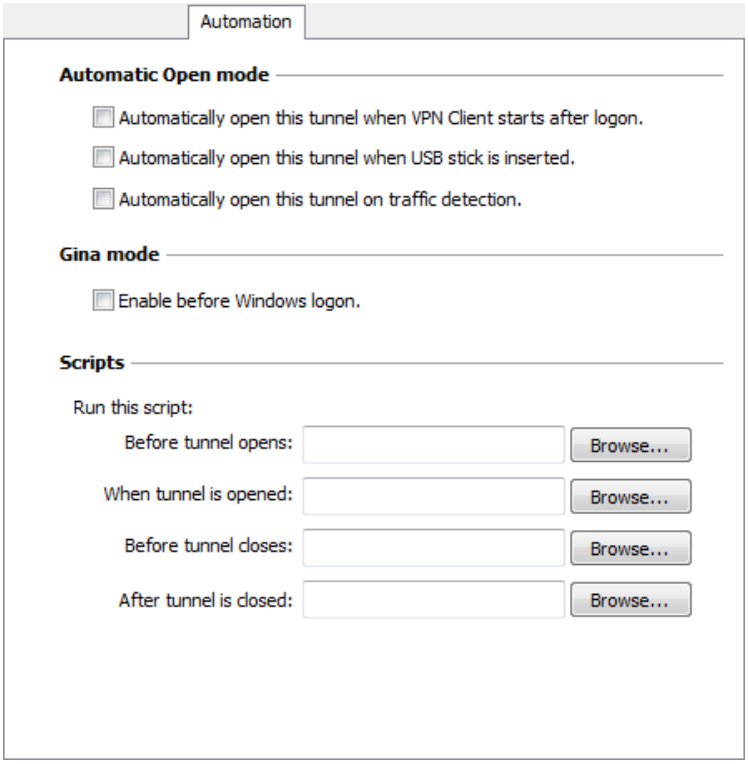
5.5.1.6 Certificate

See chapter "Managing Certificates".

5.5.1.7 Remote Sharing

See chapter "Remote Desktop Sharing".

5.6 Automation



Automatic Open Mode	3 modes are available for automatic opening of the tunnel: 1/ The tunnel opens automatically when the VPN Client starts (1). 2/ The tunnel is part of a configuration on USB (see "USB mode"), and it is opened automatically USB drive is plugged in (2). 3/ The tunnel opens automatically on traffic detection to an IP address belonging to the remote network (see "How to configure the address of the remote network").
Gina Mode (3)	Gina opens the tunnel before Windows logon. By checking this option, the tunnel appears in the VPN Gina and can be opened before Windows logon.
Scripts	Command lines can be configured to be executed: - Before opening the tunnel - After the opening of the tunnel - Before closing the tunnel - After closing the tunnel

(1) This option allows you to configure to open a tunnel automatically when double-click on the file ".tgb": Select the option "Automatically open this tunnel when the VPN Client starts," save and export the configuration file "tunnel_auto.tgb" leave the VPN Client. By double-clicking on the file "tunnel_auto.tgb" VPN Client starts and the tunnel opens automatically.

(2) By extension, this option is also used to configure a tunnel to open automatically when a Smartcard or a token containing the certificate used by the VPN tunnel is plugged in. See chapter "Use a VPN Tunnel with a Certificate from a SmarCard".

(3) Gina Credential Providers in Windows Vista, Windows 7 and further.

The command line can be:
- call to a "batch" file, e.g. `"C:\vpn\batch\script.bat"`
- execution of a program, e.g. `"C:\Windows\notepad.exe"`

- opening a web page, e.g. "`http://192.168.175.50`"
- etc...

There are many possible applications for this function:

- Creating a semaphore file when the tunnel is open, so that a third-party application can detect when the tunnel is opened
- Automatic opening an intranet server, once the tunnel opens
- Cleaning or checking a configuration before the opening of the tunnel
- Check the computer (anti-virus updated, correct versioning of application, etc.) before the opening of the tunnel
- Automatic cleaning (deleting files) of a work area on the computer before closing the tunnel
- Application counting openings, closings and duration of VPN tunnel sessions
- Changing the network configuration, once the tunnel opened and restoration of the initial network configuration after closing the tunnel
- etc.

6 IPv4 and IPv6 ready

TheGreenBow VPN Client supports heterogeneous IPv4 and IPv6 networks on the LAN and WAN sides, either on corporate or user home networks.

The feature 'Auto' (for IPv4/IPv6) enables you to support those complex environments.

The IPv4 and IPv6 ready capability is available throughout the software, and the setup is available in the following chapters:

- IPv4/IPv6 setup for IPsec VPN tunnel with IKEv1 in Phase 1 and Phase 2
- IPv4/IPv6 setup for IPsec VPN tunnel with IKEv2 in Child SA

For SSL tunnel, the discovery and configuration is fully automatic, no settings required. Additionnaly, one SSL tunnel can support IPV4 and IPV6 traffic in the VPN tunnel at the same time (i.e. you don't need two VPN tunnels, like you would with IPsec/IKE).

Depending on the mix of IPv4 and IPv6 networks you might use one of the following VPN configuration guide lines:

- IPsec with IKEv1 Phase1-Authentication: Always select 'Auto' mode for IPv4/IPv6. If the corporate gateway restricts to IPv4 on WAN side then select IPv4 in the IPsec VPN Client Phase1.
- IKEv1-Phase2-IPsec or IKEv2-Child SA: Always select IPv4 if your corporate network is IPv4 and select IPv6 if your corporate network is IPv6.

7 Managing Certificates

TheGreenBow VPN Client is fully integrated with most PKI solution in the market.

The software implements a set of features for different certificates storage (files, Windows Certificate Store, Smartcard and Token).

TheGreenBow VPN Client supports X509 certificates.
TheGreenBow VPN Client uses the certificate files formats, PKCS12, PEM.
TheGreenBow VPN Client supports the following storage devices: Windows Certificate Store (CSP), Smartcard or Token (PKCS11 CSP).
The VPN Client supports user certificates (VPN Client side) as well as the VPN Gateway certificates.

Note: TheGreenBow VPN Client cannot create certificates. However, the VPN Client can manage certificates created by third-party software, and stored on a Smartcard, token or in the Windows Certificate Store. VPN Client can also import certificates in the VPN security policy.

TheGreenBow VPN Client also enables to refine Smartcard, Token and Certificate management through a set of "PKI options". Example : automatic smartcard reader recognizing, certificate filters, etc.
See chapter "PKI Options" below.

7.1 Setup a Certificate

7.1.1 Select a certificate ("Certificate" tab)

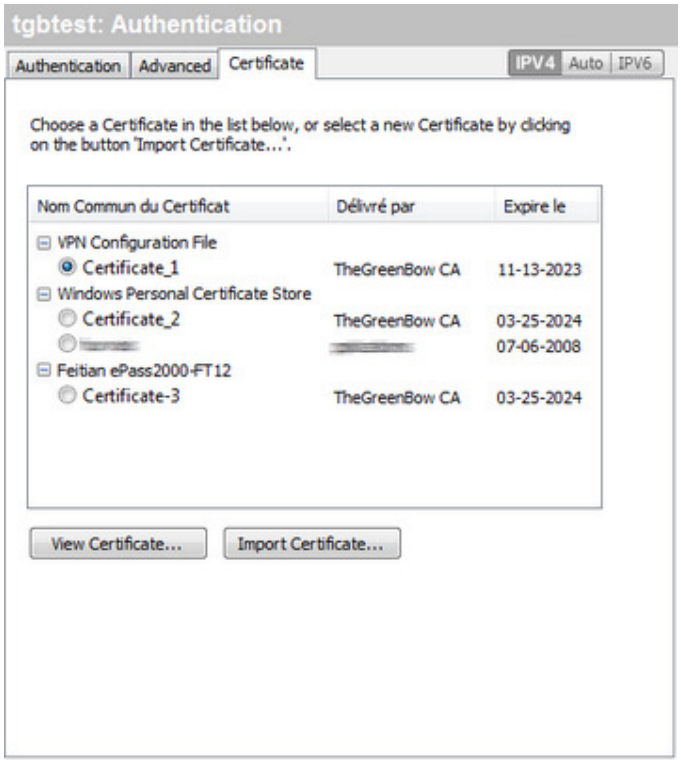
VPN Client allows you to assign a user certificate to a VPN tunnel.
There can be only one certificate per tunnel, but each tunnel can have its own certificate.

VPN Client allows you to select a certificate stored:
- In the VPN Configuration file (see "Import Certificate")
- In the Windows certificate store (see "Windows Certificate Store")
- On a Smartcard or a token (see "Configure a Smartcard or Token")

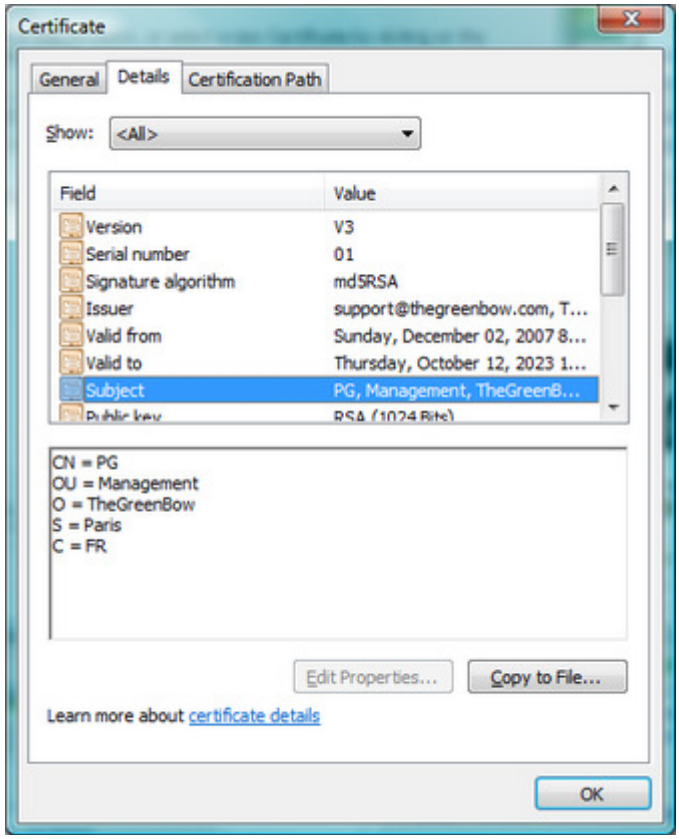
The "Certificate" tab will list all relevant media available on the computer, which contain certificates. If a media does not have a certificate, it is not displayed in the list (e.g. if the VPN Configuration file contains no certificate, it does not appear in the list).

By clicking one of the media, the list of certificates it contains is displayed.

Click on the desired certificate to assign to the VPN tunnel.



Once the certificate is selected, the button "View Certificate" allows to view the details of the certificate.



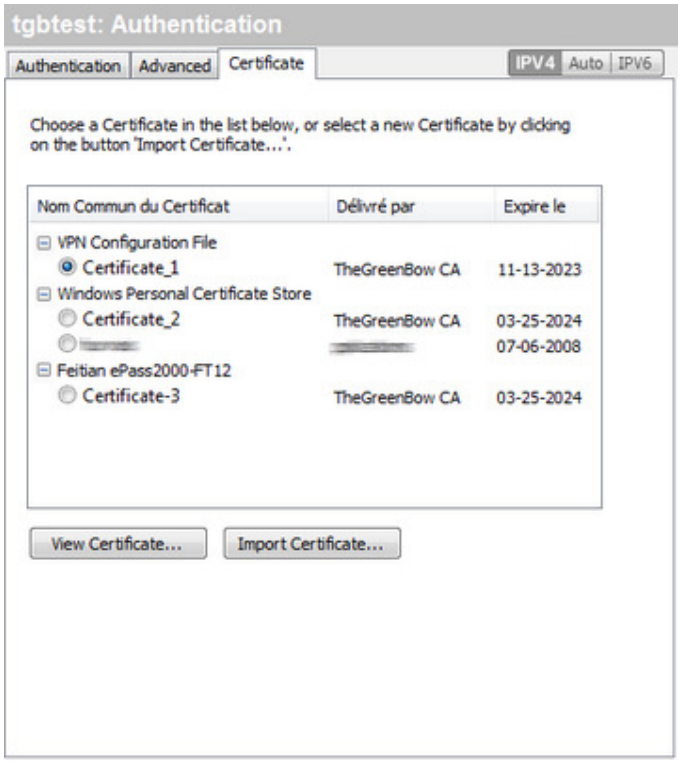
Note: Once the certificate is selected, the Phase 1 type of Local ID will automatically switch to "Subject X509" (aka DER ASN1 DN), and the certificate subject is used as the default value of this "Local ID".

7.1.2 Define a SmartCard or Token

The list of Smartcard readers and Tokens compatible and/or qualified with TheGreenBow VPN Client is available on the TheGreenBow website at: www.thegreenbow.com/vpn/vpn_token.html

Once a reader is properly installed with the smartcard inserted, or when a token is available, it is identified in the list of media of certificates in the selected "Certificate" tab.

To select a certificate, click the Smartcard or Token that contains it, and select the correct certificate:



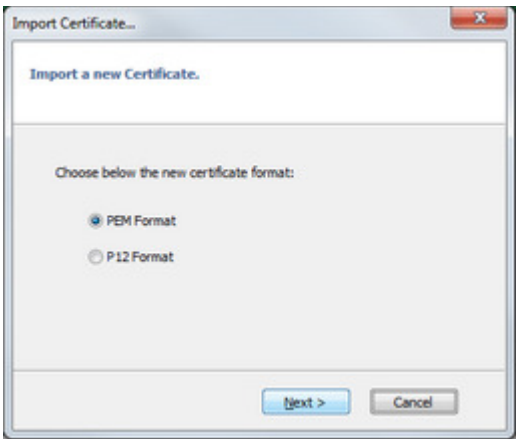
In case your Token or Smartcard is not recognized, please refer to our "Token and Smartcard User Guide" (section add a new ATR) available at: http://www.thegreenbow.com/vpn/vpn_token.html

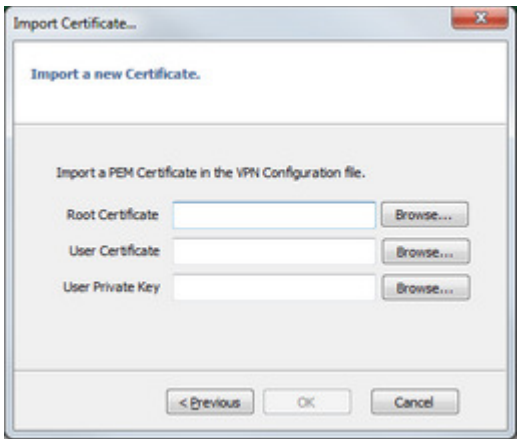
7.2 Import a certificate

TheGreenBow VPN Client can import certificates in the VPN security policy with PEM or PKCS12 format. The advantage of this solution, less secure than using the Windows certificate store or a Smartcard, is to enable the easy and fast deployment of certificates.

7.2.1 Import a PEM certificate

1/ In the "Certificate" tab of either a Phase 1 (IKEv1), IKE auth (IKEv2) or SSL, click on "Import a Certificate..."
2/ Select "PEM Format"
3/ Select ("Browse") root certificates, user and private key to import
Note: The file with the private key must not be encrypted.
4/ Validate

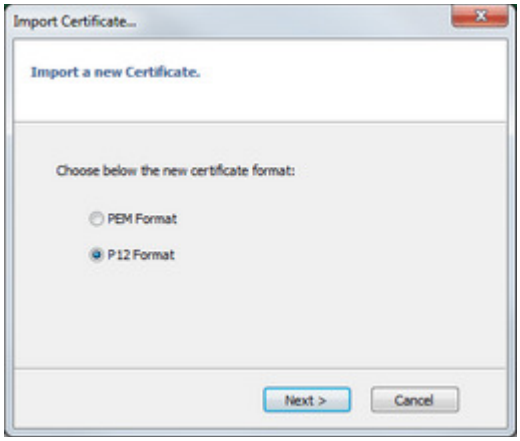


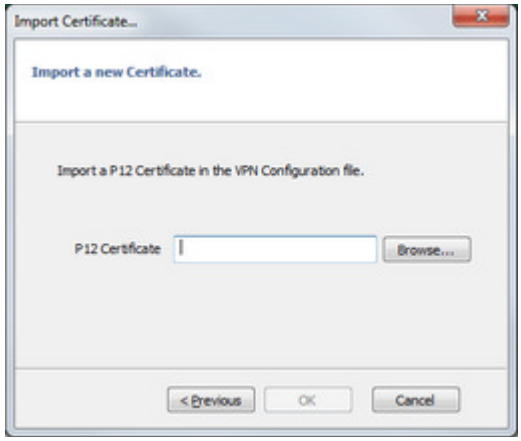


The certificate appears and is selected from the list of certificates on the "Certificate" tab.
Save the VPN security policy: The certificate is stored in the VPN security policy.

7.2.2 Import a PKCS12 certificate

1/ In the "Certificate" tab of either a Phase 1 (IKEv1), IKE auth (IKEv2) or SSL, click on "Import a Certificate..."
2/ Select "Format P12"
3/ Browse to import the PKCS12 certificate
4/ If it is protected by a password, enter the password and validate





The certificate appears and is selected from the list of certificates on the "Certificate" tab.
Save the VPN security policy: The certificate is stored in the VPN security policy.

7.3 Using Windows Certificate Store

For a certificate of Windows Certificate Store to be identified by the VPN Client, it must meet the following specifications:

- The certificate must be certified by a certification authority (excluding the self-signed certificates)
- The certificate must be located in the Certificates store "Personal" (It represents the personal identity of the user who wants to open a VPN tunnel to the corporate network).

Note: To manage certificates in the Windows Certificate Store, Microsoft offers a standard management tool "certmgr.msc." To run this tool, go to the Windows menu "Start," then in the "Search programs and files", enter "certmgr.msc."

7.4 Use a VPN Tunnel with a Certificate from a Smartcard

When a VPN tunnel is configured to use a certificate stored on Smartcard or token, a PIN code to access to the Smartcard is required to the user when tunnel opens.

If the Smartcard is not inserted, or if the token is not available, the tunnel does not open.
If the PIN code entered is incorrect, the VPN Client notifies the user that has 3 consecutive attempts before locking out the Smartcard.

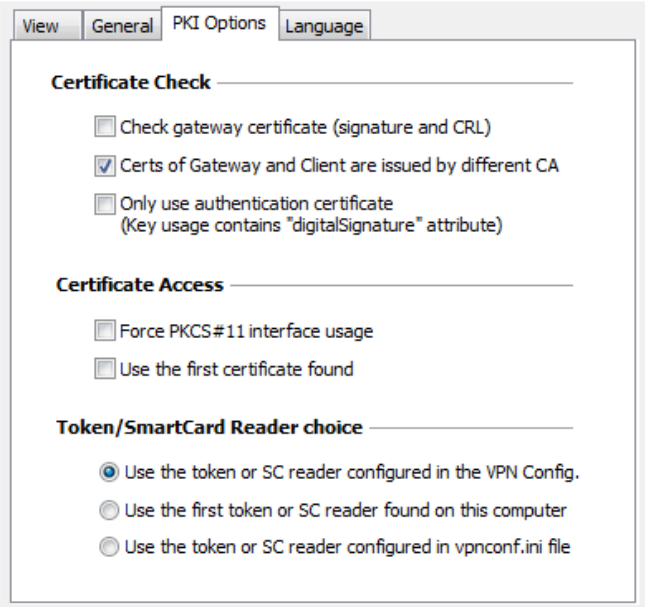
The VPN Client implements a mechanism for automatically detecting the insertion of a Smartcard.
Thus, the tunnels associated with the certificate contained on the Smartcard are opened automatically upon inserting the Smartcard. Conversely, removal of the Smartcard automatically closes all associated tunnels.
This functionality is achieved by checking the option "Open tunnel automatically when the USB drive is inserted" (see chapter "IPsec Advanced").

7.5 PKI Options

TheGreenBow VPN Client enables to refine Smartcard, Token and Certificate management through a set of "PKI options".

This feature is only available with the PREMIUM release of TheGreenBow VPN Client.

The "PKI Options" menu is available by clicking on the "Tools > Options..." menu of the Configuration Panel.



For details and examples on how to specify smartcard, token and certificate access with the "PKI options" set, please refer to our dedicated user guide: "Token and Smartcard User Guide" available on www.thegreenbow.com/vpn/vpn_token.html

8 Import, Export VPN Security Policy

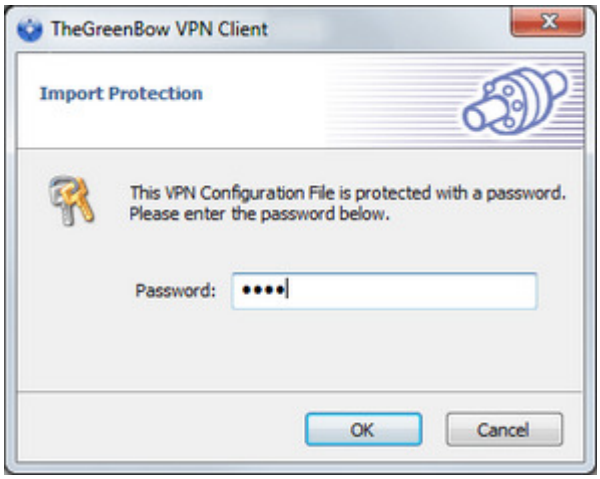
8.1 Import a VPN security policy

TheGreenBow VPN Client can import a VPN security policy in different ways:
- From the menu "Configuration" > "Import" in the Configuration Panel
- By drag and drop of a VPN Configuration file (file ".tgb") onto the Configuration Panel
- By double-clicking a VPN Configuration file (file ".tgb")
- By using the command line option "/import" (1)

(1) The use of command line options of the software is described in the document "Deployment Guide". All the options available for importing a VPN security policy are detailed there: "/import", "/add", "/replace" or "/importonce."

Note: The VPN configuration files have the following extension ".tgb".

To import a VPN configuration, the user shall say if he wants to add new Configuration to the current VPN Configuration, or if he wants to replace (overwrite) the current configuration with the new VPN Configuration. If the VPN security policy has been saved with a password, it will be asked to the user.



If the VPN security policy has been exported with integrity check (see chapter "Exporting a VPN Security Policy") and it has been corrupted, a message alerts the user, and the software does not import the Configuration.

Note: If VPN tunnels added have the same name as the VPN tunnel in current configuration, they are automatically renamed during import (adding an increment between brackets).

Importing Global Parameters

If during import, the user selects "Replace", or if the current configuration is empty, the Global Parameters from the imported configuration replace VPN Global Parameters from the current configuration.
If during import, the user chooses "Add", Global Parameters of the current VPN configuration are kept.

Import user choice	Current configuration is empty	Current configuration not empty
Add	Global Parameters replaced by the new ones	Global Parameters kept
Replace	Global Parameters replaced by the new ones	Global Parameters replaced by the new ones

8.2 Exporting a VPN security policy

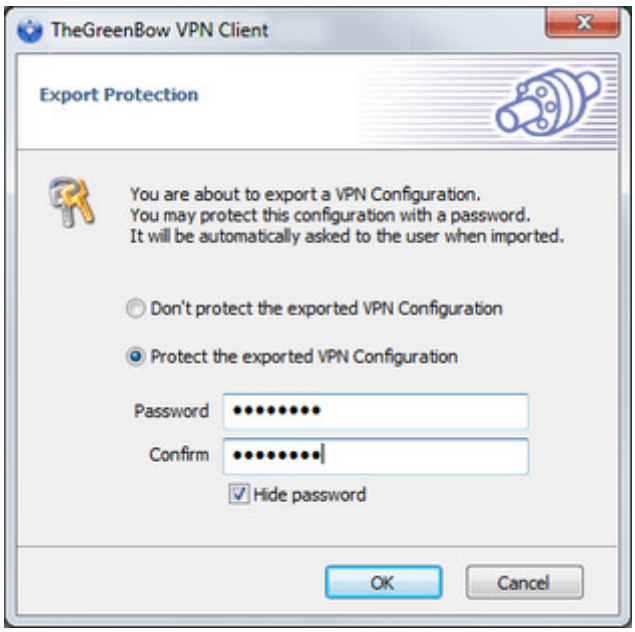
TheGreenBow VPN Client can export a VPN security policy in different ways:

- In the menu "Configuration" > "Export" from the Configuration Panel: The entire VPN security policy is exported.
- Via right click on the root of the tree of the Configuration Panel (menu choose "Export"): The entire VPN security policy is exported.
- Via right click on any items in the tree (then choose "Export"): the item selected and depending ones are exported (e.g. Phase 1 and all associated Phase 2, or Phase 2 and the associated Phase 1)
- By using the command line option "/export" (1)

(1) The use of command line options of the software is described in the document "Deployment Guide". All the options available for exporting a VPN security policy are detailed there: "/export" or "/exportonce".

Note: The VPN configuration files have the following extension ".tgb".

Whatever the method used, the export operation begins with the choice of protection for the exported VPN security policy: It can be exported protected (encrypted) by a password, or exported "readable" (clear). When configured, the password is required from the user at the time of import.



Note: whether exported encrypted or "clear", the exported configuration integrity can be protected.

When exported VPN security policy integrity is protected, and subsequently corrupted, a warning message notifies the user during import, and the software does import the configuration (see chapter "Importing a VPN security policy" above).

8.3 Merge VPN security policies

It is possible to merge multiple security policies in a single VPN, by importing all VPN configurations, and selecting "Add" for each import (see chapter "Importing a VPN security policy").

8.4 Split VPN security policies

Using different export options (e.g. export a Phase 1 with all associated Phase 2 or export a single tunnel), it is possible to split a VPN security policy in many "sub-configurations" (See chapter "Exporting a VPN security policy").

This technique can be used to deploy VPN security policies on a large pool of computers: you can derive, the VPN policies associated with each computer from a common VPN policy, before distributing to each user for import.

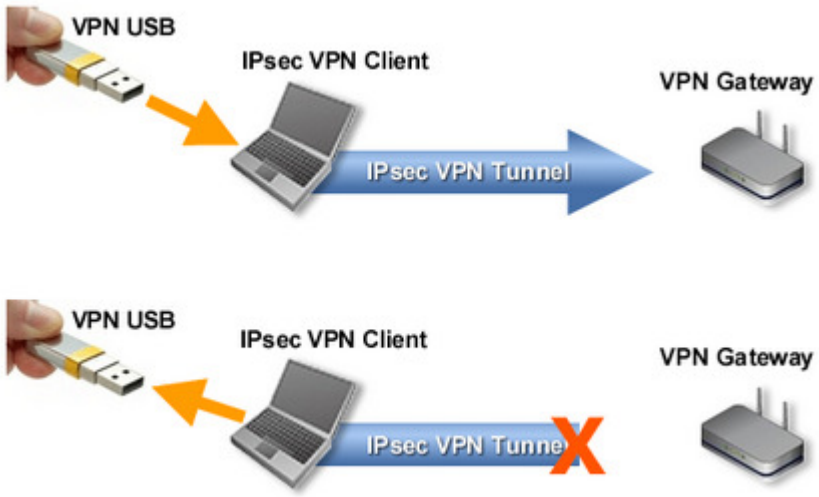
9 USB Mode

9.1 What is the USB Mode?

TheGreenBow VPN Client provides the ability to protect the VPN security policy (VPN Configuration, pre-shared key, certificate) on a USB drive.

The advantages of this mode are:

1/ The security policy is no longer stored on the computer but on a removable media (VPN Configuration stored is encrypted and protected with password)
2/ The VPN Client automatically detects USB drive containing a VPN Configuration. It will automatically load the configuration, and automatically opens the configured tunnel.
3/ When the USB drive is removed, the tunnel is automatically closed (and previous VPN Configuration restored)



In this document, the USB drive containing the VPN security policy is called "USB VPN Drive".

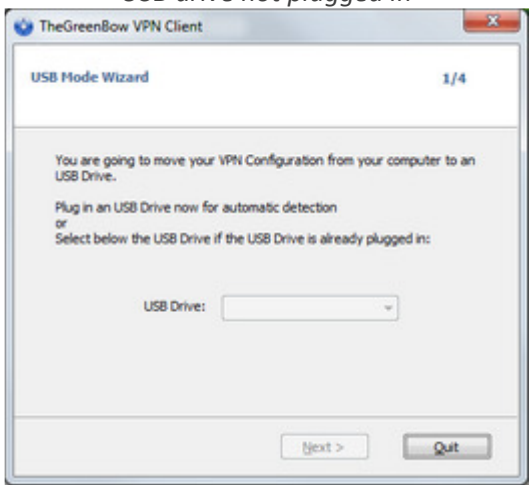
9.2 USB Mode settings

The USB mode can be configured via the setup wizard accessible via the Configuration Panel menu "Configuration" > "Move to USB drive".

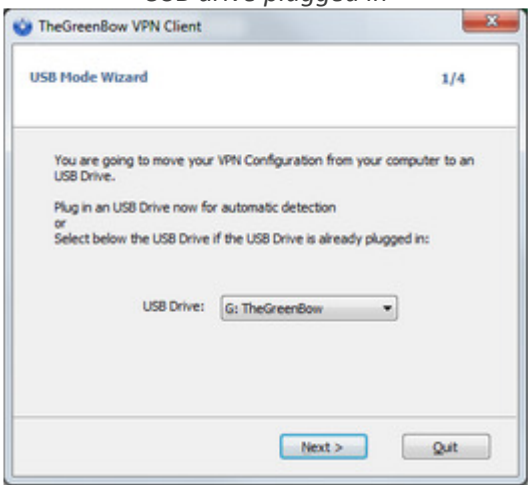
9.2.1 Step 1: Select the USB drive

Select the USB Drive to be used to protect the VPN security policy.
If a USB Drive is already plugged in, it is automatically shown in the list of USB drives available.
Otherwise, simply plug in the USB drive.

USB drive not plugged in



USB drive plugged in



Note: The USB mode allows the protection of a single VPN Configuration on a USB drive. If a VPN Configuration is already present on the USB drive plugged in, a warning message is displayed.

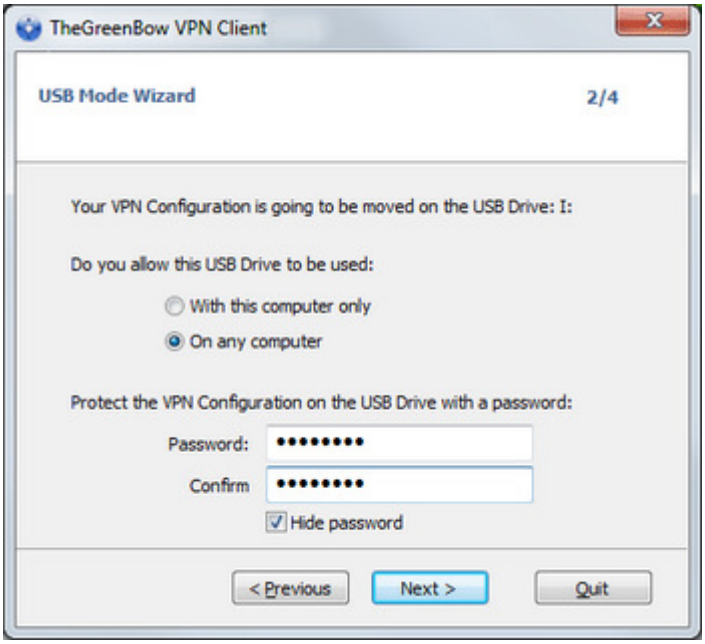
Note: When a USB drive plugged in is empty and it is the only one plugged in on the computer, the wizard automatically moves to step 2.

9.2.2 Step 2: Protection USB VPN security policy

Two protections are available:

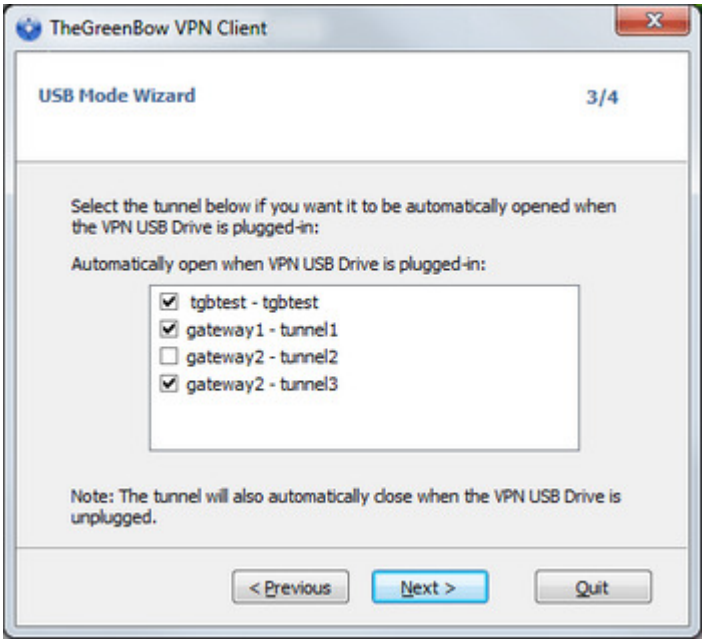
1/ Association with the current computer:
The USB VPN policy can be uniquely associated to the current computer. In this case, the USB VPN can only be used on that computer. Otherwise (the USB is not associated with a particular computer), USB VPN can be used on any computer with a VPN Client.

2/ Password protection:
The USB VPN security policy can be protected by password. In this case, the password is required each time you plug in the VPN USB drive.



9.2.3 Step 3: Open tunnel automatically

The wizard allows you to configure tunnels that will automatically open each time you insert the USB VPN.



9.2.4 Step 4: Summary

The summary is used to validate the correct setting of the USB VPN.

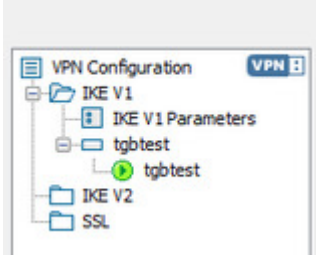
After validation of this last step, the VPN security policy is transferred to the USB.
It remains active as long as the USB is plugged in. Extraction of the USB VPN, VPN Client returns an empty VPN Configuration.

9.3 Use the USB Mode

When TheGreenBow VPN Client is launched, with a VPN security policy loaded or not, plug in the USB VPN. A popup window will ask to activate the USB mode.

After validation, the USB VPN policy is automatically loaded and, if applicable, tunnel(s) automatically open. The USB mode is identified in the Configuration Panel by a "USB Mode" icon at the top right of the tree.

Configuration Panel



Upon USB VPN drive removal the tunnel(s) are closed, and the previous VPN policy is restored.

Note: The VPN Client takes into account only one USB VPN at a time. Other USB VPN drives are not taken into account as long as the first one is plugged in.

Note: The import feature is disabled in USB mode.

In USB mode, the USB VPN security policy can be changed. Changes to the VPN policy is saved on the USB VPN.

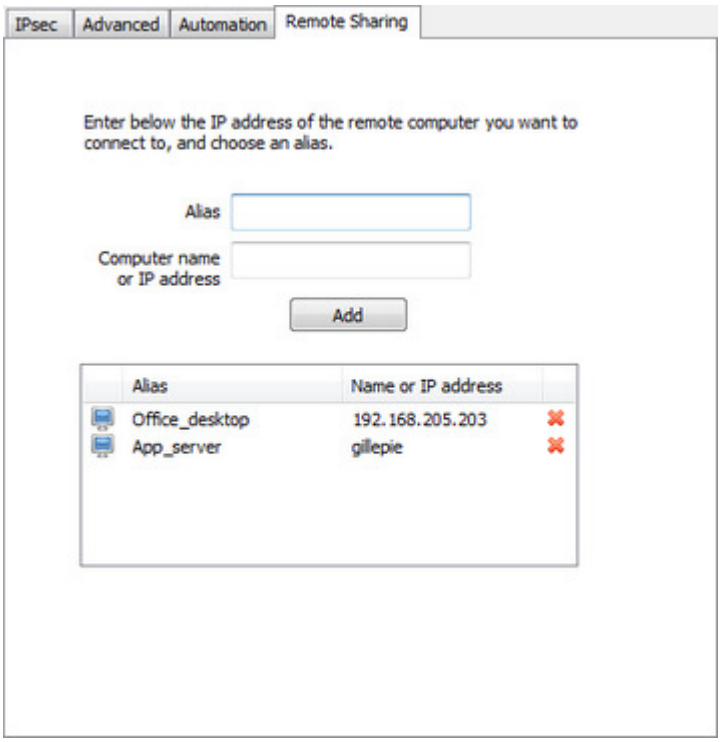
Note: The VPN Client does not provide a direct option to change the password and association to the computer. To change them, use the following procedure:
1/ Plug in the USB VPN drive
2/ Export VPN Configuration
3/ Remove the USB VPN drive
4/ Import VPN Configuration exported in step 2
5/ Restart Wizard USB mode with this configuration and the new desired settings.

10 Remote Desktop Sharing

TheGreenBow VPN Client allows to configure the "Remote Desktop" logon in the VPN tunnel with one click only: With one click, the VPN tunnel opens to the remote network, and the RDP (Windows Remote Desktop Protocol) session is automatically opened on the remote computer.

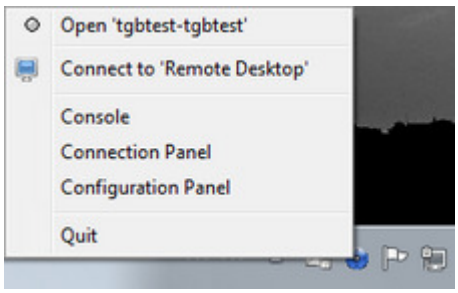
10.1 Configuring the Remote Desktop Sharing

1/ Select the VPN tunnel in which the "Remote Desktop" session will be opened.
2/ Select the "Remote Sharing" tab.
3/ Enter an alias for the connection (this name is used to identify the connection in the different software menus), and enter either the IP address or the name of the machine of the remote computer.
4/ Click on "Add": The Remote Desktop Sharing session is added to the list of sessions.



10.2 Using the Remote Desktop Sharing

1/ Right click on the icon in the taskbar: the menu is displayed
2/ Click on the "Connect to Remote Desktop" in the menu in the taskbar: the VPN tunnel opens and the desktop sharing session opens.



11 GINA Mode (VPN Tunnel before Windows logon)

The GINA mode enables to open VPN tunnels before Windows logon.

When a tunnel is configured in "GINA mode", a tunnel opening window (similar to the Connection Panel) is displayed on the Windows logon screen. It allows to manually open the VPN tunnel.

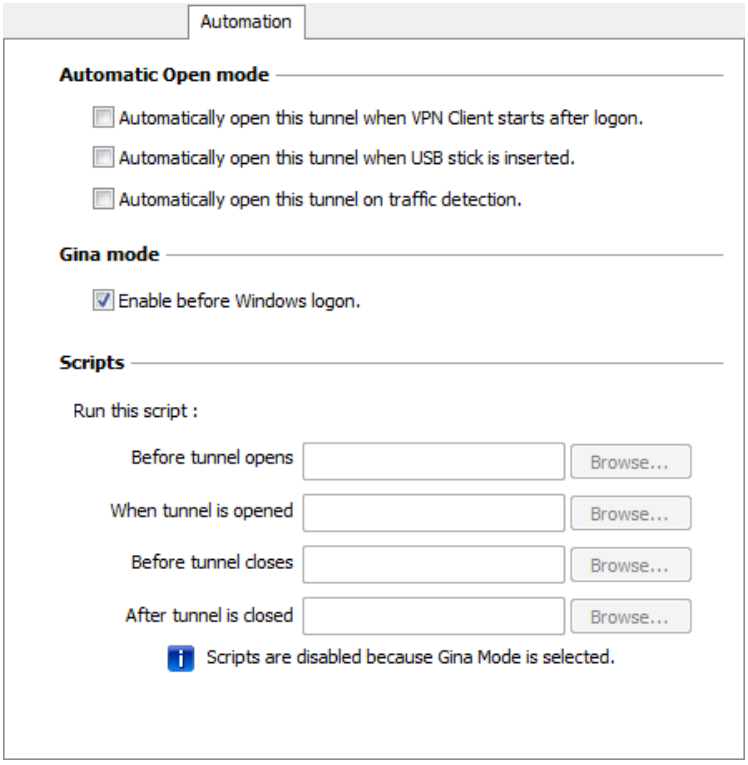
The GINA mode is available for all the VPN protocols (IKEv1, IKEv2 and SSL). It can be set in the "Automation" tab of each VPN tunnel.

11.1 Configuring the GINA Mode

11.1.1 VPN tunnel opening manually

1/ Select the VPN tunnel in the VPN tree of the Configuration Panel (IKEv1 > Phase2, IKEv2 > ChildSA or SSL > TLS)
2/ Select the "Automation" tab
3/ Select the option: "Gina Mode" > "Enable before the Windows logon"

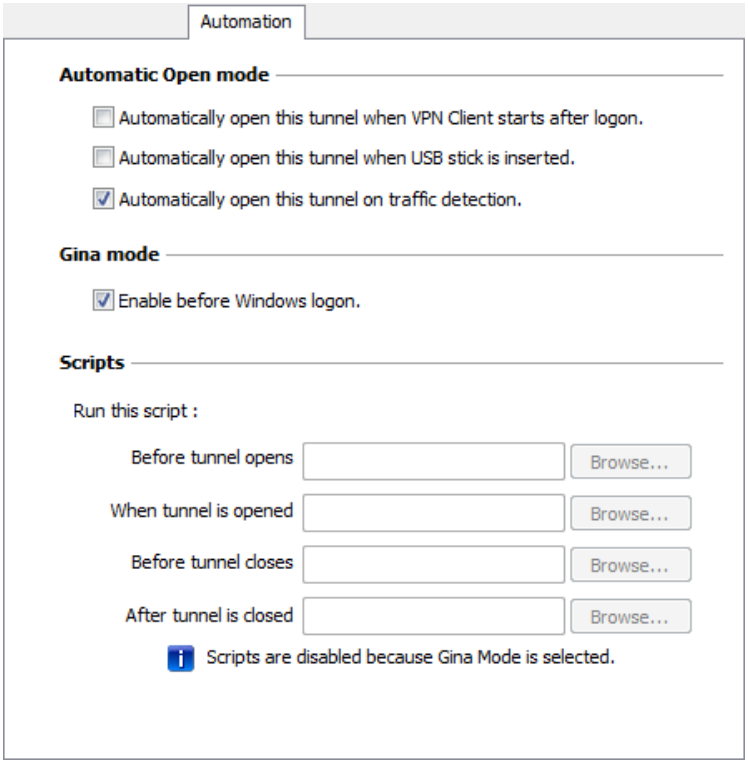
Note: An alert reminds that the script feature is not available for a tunnel in Gina mode.



11.1.2 VPN tunnel opening automatically

1/ Select the VPN tunnel in the VPN tree of the Configuration Panel (IKEv1 > Phase2, IKEv2 > ChildSA or SSL > TLS)
2/ Select the "Automation" tab
3/ Select the option: "Gina Mode" > "Enable before the Windows logon"
4/ Select the option: "Automatically open this tunnel on traffic detection"

Note: An alert reminds that the script feature is not available for a tunnel in Gina mode.



11.2 Using the GINA Mode

When the VPN tunnel is configured in GINA mode, the window of the GINA tunnels opening is displayed on the Windows logon screen. The VPN tunnel is automatically opened if configured to do so.

VPN Tunnel in GINA mode can perfectly implement an X-Auth Authentication (the user must then enter his login / password), or a certificate authentication (the user must then enter the PIN access code to the Smartcard).

Warning: If two tunnels are configured in GINA Mode, and one of them opens automatically, it is possible that both tunnels are opened automatically.

Note: In order to get the "Automatically open on traffic detection" option operational, after opening of a Windows session, the "Enable before the Windows logon" option should not be checked.

Limitation: Scripts and USB Mode are not available for VPN tunnels in GINA mode.

Security considerations:

A tunnel configured in GINA Mode can be opened before the Windows logon, therefore by any user of the computer. It is strongly recommended that you configure an authentication, strong whenever possible, for a tunnel in Gina Mode, e.g. an X-Auth Authentication, or preferably a certificate authentication, if possible on removable media.

12 Options

12.1 View

TheGreenBow VPN Client software allows to protect access to the VPN security policy by a password. From this point forward, this password is called "Administrator password".

The provided protection applies on one hand to the Configuration Panel access (regardless of which way the Configuration Panel is opened, the password is requested), on the other hand to all possible operations on the VPN security policy: changes, registration, import, export.

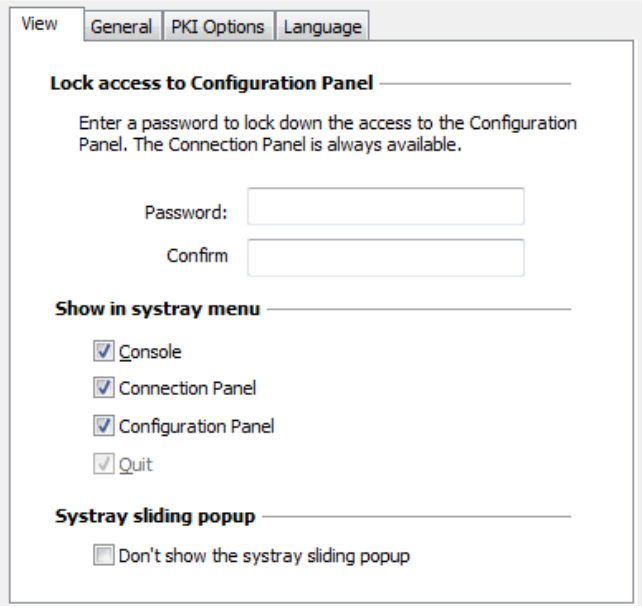
Thus, any import of a VPN security policy will be enabled if the right Administrator password is provided. These security options are detailed in the "Deployment Guide" document i.e. tgbvpn_ug_deployment.pdf.

12.1.1 Access control to the VPN security policy

Any access to the VPN security policy (reading, change, application, import, export) can be protected by a password. This protection also applies to transactions done via the command line.

To ensure the integrity and confidentiality of VPN security policy, it is recommended to implement this protection.

The protection of the VPN security policy is configured via "Tools" > "Options" > "View" tab.



Once a password is configured, opening the Configuration Panel or accessing the VPN security policy (import substitution, addition) is always conditioned by entering this password:

- when the user clicks on the icon in the taskbar
- when the user selects the Configuration Panel menu in the icon menu in the taskbar
- when the user clicks on the [+] button of the Connection Panel
- when importing a new VPN security policy via the command line
- during a software update.

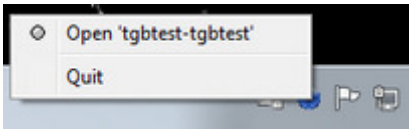
By combining this option with other options to limit the display of software, the administrator can configure the software in almost invisible and non-editable mode.

To remove the protection via password, empty both "Password" and "Confirm" fields, then confirm.

Note for the IT Manager: The protection of the VPN security policy can also be configured via the set up command line. This option is described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

12.1.2 Hide menus

The options on the "View" tab of the "Options" window also allow to hide all software interfaces, by removing from the taskbar menu the "Console", "Configuration Panel" and "Connection Panel" items. The menu in the taskbar is then reduced to the single list of available VPN tunnels.



Note for the IT Manager: When deploying software, all these options can be preconfigured during the installation of TheGreenBow VPN Client software. These options are described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

The "Quit" item from the taskbar menu cannot be removed via software. However, it may be removed using the installation options (see "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf).

12.2 General

12.2.1 Start mode

When the "Start the VPN Client after Windows logon" option is checked, the VPN Client starts automatically when Windows starts, after the Windows logon.

If the option is unchecked, the user must manually start the VPN Client, either by double-clicking on the desktop icon, or by selecting the start menu of the software in the Windows "Start" menu. See chapter "Windows Desktop".

12.2.2 Disabling the disconnection detection

In its generic behavior the VPN Client closes the VPN tunnel (on its side), when it finds a problem communicating with the remote VPN gateway.

In unreliable local networks, prone to frequent micro-disconnections, this feature can have drawbacks (which can go up to unable to open a VPN tunnel).

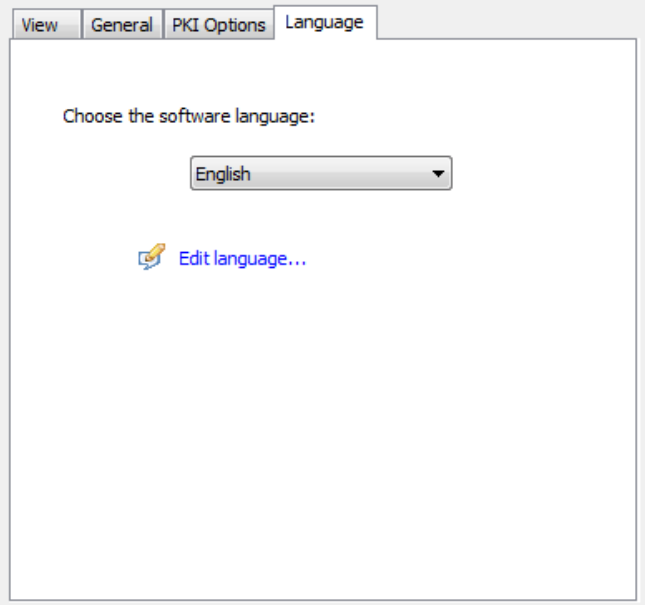
By checking the "Disable disconnection detection" box, the VPN Client avoids closing tunnels when a disconnection is detected. This ensures excellent stability of the VPN tunnel, including unreliable local networks, typically wireless networks like WiFi, 3G, 4G, or satellite.

12.3 Managing languages

12.3.1 Choosing a language

TheGreenBow VPN Client can be run in multiple languages.
It is possible to change the language while the software is running.

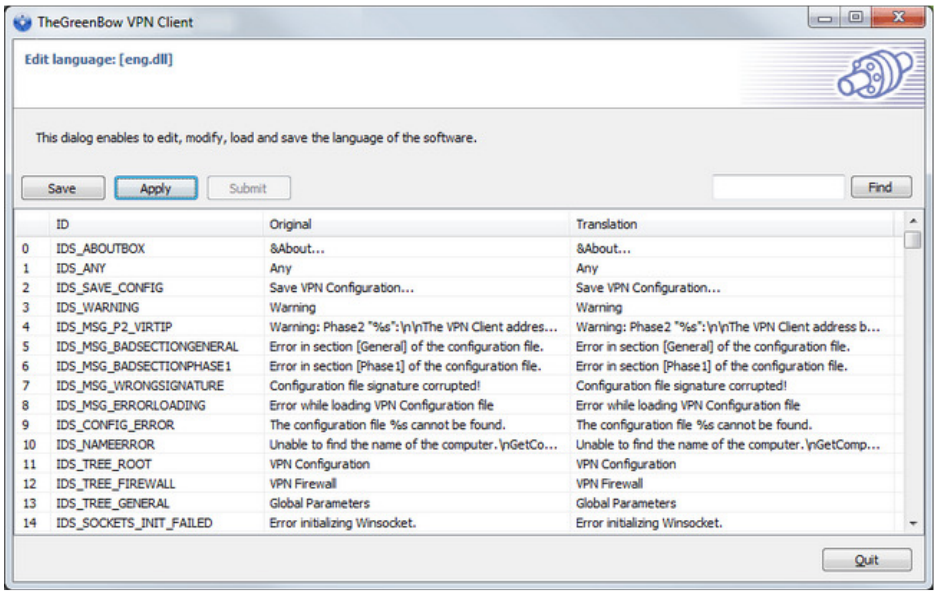
To select another language, open the "Tools" > "Options" menu and select the "Language" tab.
Choose the desired language from the proposed drop-down list:



The list of languages available in the standard software is provided in the appendix to the chapter "List of available languages".

12.3.2 Modifying or creating a language

TheGreenBow VPN Client also allows to create a new translation or make changes to the language that is being used, then to test these changes dynamically via an integrated translation tool.
In the "Language" tab, click on the "Edit language..." link; the translation window is displayed:



The translation window is divided into four columns which indicate respectively the number of the string, its ID, its translation in the original language, and its translation into the selected language.

The translation window allows to:
1/ translate each string by clicking on the corresponding line
2/ search for a given string in any column of the table ("Search" input field, then use the "F3" key to run through all occurrences of the searched string)
3/ save the changes
Any language modified or created is saved in a "lng" file
4/ immediately apply a change to the software: this feature allows to validate in real time whether any string is pertinent or properly displayed ("Apply" button)
5/ send to TheGreenBow a new translation ("Send" button).

The name of the language file that is being edited is recalled in the header of the translation window.

Note: Any translation sent to TheGreenBow is published, after checking, on the TheGreenBow site, then added to the software, usually in the published official version, following receipt of the translation.

Additional notes:
Characters or following sequences of characters should not be changed during the translation:

"%s"	will be replaced by the software with a string
"%d"	will be replaced by the software with a number
"\n"	indicates a carriage return
"&"	indicates that the next character should be underlined
"%m-%d-%Y"	indicates a date format (here the format U.S.: month-day-year) modify this field only if knowledge of the format in the translated language.

Note: "IDS_SC_P11_3" string must be used without modification.

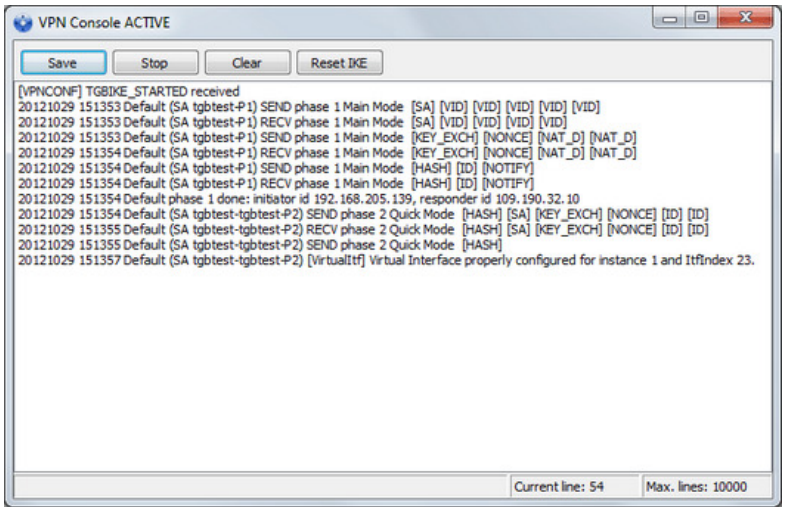
13 Console and Trace Mode

TheGreenBow VPN Client offers two tools that generate logs:
1/ The "Console" provides information and steps to open and close the tunnels (IKE messages for most of them)
2/ The "Trace Mode" asks each software component to produce its activity's log.

Both tools are designed to help the network administrator to diagnose a problem during tunnels opening, or TheGreenBow support team in identifying software's incidents.

13.1 Console

Console can be displayed as follows:
- Menu "Tools" > "Console" in the Configuration Panel
- Ctrl+D shortcut when the Configuration Panel is open
- In the software menu in the taskbar, select "Console"



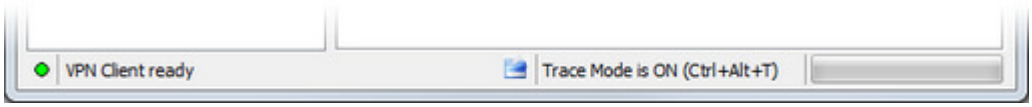
The Console features include:
- Save: Save in a file all traces displayed in the window
- Start / Stop: Start / stop the capture of recording
- Delete: Delete the content of the window
- Reset IKE: Restart the IKE service.

13.2 Trace Mode

Trace Mode is activated by the shortcut: Ctrl+Alt+T

Switching to Trace Mode does not require to restart the software.

When Trace Mode is enabled, each component of TheGreenBow VPN Client generates logs of its activity. The generated logs are stored in a folder accessible by clicking the blue "Folder" icon in the status bar in the Configuration Panel.



14 Recommendations for Security

14.1 General recommendations

To ensure an appropriate level of security, conditions to implement and use must be met as follows:

- The system administrator and security administrator, respectively responsible for the installation of software and the definition of VPN security policies, are considered trusted persons.
- The software user is a person trained in its use. In particular, he/she shall not disclose the information used for authentication to the encryption system.
- The VPN gateway to which the VPN Client connects allows to track the VPN activity and to show malfunctions or violations of security policies if they occur.
- The user's workstation is healthy and properly administered. It has an up-to-date anti-virus, and is protected by a firewall.
- The bi-keys and certificates used to open the VPN tunnel are generated by a trusted certification authority.

14.2 VPN Client administration

It is strongly recommended to protect access to the VPN security policy by a password and limit the visibility of the software to the end user, as detailed in chapter "**Access control to the VPN security policy**".

It is also recommended to set this protection at the time of installation, via the installation options described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

It is recommended to ensure that users are using the VPN Client in a "user" environment and try, as much as possible, to limit the use of the operating system with administrator rights.

It is recommended to keep the "Starting the VPN Client with Windows session" mode (after the Windows logon), which is the default installation mode.

14.3 Configuring VPN security policy

Use Authentication

The features of user authentication proposed by the VPN Client are described below, from the weakest to the strongest.

In particular, please note that authentication via pre-shared key is easy to implement, however it allows any user with access to the computer to open a tunnel without authentication check.

User authentication type	Strength
Pre Shared Key	weak
Static X-auth	
Dynamic X-Auth	
Certificate stored in the VPN security policy	
Certificate in the Windows Certificate Store	
Certificate on Smartcard or Token	strong

IKE V1 Protocol

It is recommended to set the "Main Mode" rather than "Aggressive Mode". See chapter "**Authentication Advanced**".

Gina Mode

It is recommended to add a strong authentication to any tunnel in Gina Mode.

15 Contact

Information and update are available at: **www.thegreenbow.com**

Technical support via email at: **support@thegreenbow.com**

Sales via email at: **sales@thegreenbow.com**

16 Annex

16.1 List of available languages

Code	Language	Code ISO 639-2
1033 (default)	English	EN
1036	French	FR
1034	Spanish	ES
2070	Portuguese	PT
1031	German	DE
1043	Dutch	NL
1040	Italian	IT
2052	Simplified Chinese	ZH
1060	Slovenian	SL
1055	Turkish	TR
1045	Polish	PL
1032	Greek	EL
1049	Russian	RU
1041	Japanese	JA
1035	Fins	FI
2074	Serbian	SR
1054	Thai	TH
1025	Arabic	AR
1081	Hindi	HI
1030	Danish	DK
1029	Czech	CZ
1038	Hungarian	HU
1044	Norwegian	NO
1065	Persian	FA
1042	Korean	KO

16.2 TheGreenBow VPN Client specifications

General	
Windows Versions	Windows Server 2003 32bit Windows Server 2008 32/64bit Windows Vista 32/64bit Windows 7 32/64bit Windows 8 32/64bit
Languages	Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai & Turkish
How to use	
Invisible mode	Automatic opening of the tunnel upon traffic detection Access control to the VPN security policy Possible interfaces mask
USB mode	No more VPN security policy on the computer Opening of the tunnel when inserting a configured VPN USB key Automatic closing of the tunnel when extracting the configured VPN USB key
Gina	Opening of a tunnel before Windows logon Credential providers on Windows Vista, Windows 7 and further
Scripts	Running scripts configurable upon opening and closing of the VPN tunnel
Remote Desktop Sharing	Opening of a remote computer (remote desktop) with a single click through the VPN tunnel
Connection / Tunnel	
Connection mode	Peer-to-peer (point to point between two computers equipped with VPN Client) Peer-to-Gateway (see the list of qualified VPN gateways and their configuration guides)
Tunneling Protocol	IKE based on OpenBSD 3.1 (ISAKMPD) Diffie-Hellmann DH Group 1 to 18 Full IPsec support using IKv1 and IKEv2 Full SSL/TLS support
Tunnel mode	Main mode and Aggressive mode
Config mode	Network settings automatically retrieved from the VPN gateway
Cryptography	
Encryption	Symmetric: DES, 3DES, AES 128/192/256bit Asymmetric: RSA Diffie-Hellmann: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) Hash: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512
Authentication	Admin: Securing access to VPN security policies User: − X-Auth static or dynamic (request at each tunnel's opening) − Hybrid Authentication − Pre-shared key − EAP

PKI	− Certificates: support format X509, PKCS12, PEM − Multi-support: Windows certificate store, Smartcard, Token − Certificates criteria: expiration, revocation, CRL, subject, key usage − Ability to select the Token / Smartcard interface (see **list of qualified Tokens** / Smartcard) − Automatic detection of Token / Smartcard − Access to Token / Smartcard in PKCS11 or CSP − Verification of "Client" and "Gateway" certificates
Miscellaneous	
NAT / NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode, NAT-T forced mode, automatic or off
DPD	RFC3706. Detection of non-active IKE end points.
Redundant Gateway	Management of a redundant gateway, automatically selected upon detection of DPD (inactive gateway)
Firewall	Filtering incoming / outgoing IP addresses and TCP / UDP ports
Administration	
Deployment	Options to deploy VPN policies (command line options for the set up, configurable initialization files...) Silent installation
VPN policies management	Options to import and export VPN policies Securing imports / exports by password, encryption and integrity monitoring
Automation	Open, close and monitor a tunnel from the command line (batch and scripts), startup and shutdown of software by batch file
Log and trace	IKE / IPsec logs console and trace mode activated
Live update	Checking for updates from the software
License and activation	Modularity of licenses (standard, temporary, limited duration), software activation (WAN, LAN), and deployment options (deployment of enabled software, silent activation...)

16.3 Credits and Licenses

Credits and license references.

```
/*
 * Copyright (c) 1998, 1999 Niels Provos.  All rights reserved.
 * Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>.  All rights reserved.
 * Copyright (c) 1998, 1999, 2000, 2001 Niklas Hallqvist.  All rights reserved.
 * Copyright (c) 1999, 2000, 2001, 2002, 2004 Håkan Olsson.  All rights reserved.
 * Copyright (c) 1999, 2000, 2001 Angelos D. Keromytis.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 */

/* ====================================================================
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
```

```
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

Secure, Strong, Simple

TheGreenBow Security Software